ΔΗΜΗΤΡΙΟΣ Μ. ΠΟΥΛΑΚΗΣ
ΚΑΘΗΓΗΤΗΣ ΤΜΗΜΑΤΟΣ ΜΑΘΗΜΑΤΙΚΩΝ Α.Π.Θ.

# ΑΛΓΕΒΡΙΚΟΙ ΚΩΔΙΚΕΣ

ΕΚΔΟΣΕΙΣ ΖΗΤΗ

*Κάθε γνήσιο αντίτυπο φέρει την υπογραφή του συγγραφέα*

*Για επικοινωνία με το συγγραφέα*
*poulakis@math.auth.gr*

ISBN 978-960-456-200-8



**Φωτοστοιχειοθεσία** **Π. ΖΗΤΗ & Σια ΟΕ**
**Εκτύπωση** 18ο χλμ Θεσσαλονίκης - Περαίας
**Βιβλιοδεσία** Τ.Θ. 4171 • Περαία Θεσσαλονίκης • Τ.Κ. 570 19
Τηλ.: 2392.072.222 - Fax: 2392.072.229 • e-mail: info@ziti.gr

ΕΚΔΟΣΕΙΣ ΖΗΤΗ

**www.ziti.gr**

**ΒΙΒΛΙΟΠΩΛΕΙΟ ΘΕΣΣΑΛΟΝΙΚΗΣ - ΚΕΝΤΡΙΚΗ ΔΙΑΘΕΣΗ:**
Αρμενοπούλου 27 - 546 35 Θεσσαλονίκη • Τηλ.: 2310-203.720 • Fax 2310-211.305
e-mail: sales@ziti.gr

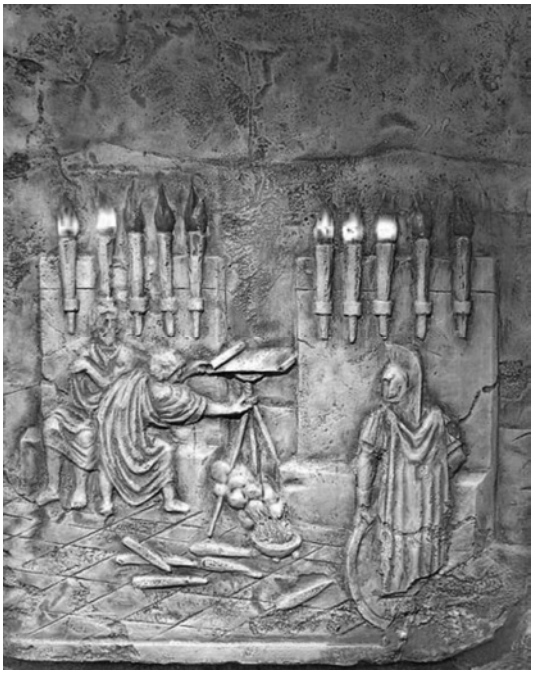
**ΒΙΒΛΙΟΠΩΛΕΙΟ ΑΘΗΝΩΝ - ΕΝΩΣΗ ΕΚΔΟΤΩΝ ΒΙΒΛΙΟΥ ΘΕΣΣΑΛΟΝΙΚΗΣ:**
Στοά του Βιβλίου (Πεσμαζόγλου 5) - 105 64 ΑΘΗΝΑ • Τηλ.-Fax: 210-3211.097

**ΑΠΟΘΗΚΗ ΑΘΗΝΩΝ - ΠΩΛΗΣΗ ΧΟΝΔΡΙΚΗ:**
Ασκληπιού 60 - Εξάρχεια 114 71, Αθήνα • Τηλ.-Fax: 210-3816.650 • e-mail: athina@ziti.gr

**ΗΛΕΚΤΡΟΝΙΚΟ ΒΙΒΛΙΟΠΩΛΕΙΟ:** www.ziti.gr

*Αφιερώνεται*
*στην πιο μεγάλη*
*αγάπη της ζωής μου*

# Οπτικός τηλέγραφος



Ο οπτικός τηλέγραφος αποτελούσε ένα από τα κύρια μέσα επικοινωνίας εξ αποστάσεων στην αρχαιότητα. Χρησιμοποιούνταν κυρίως από τον στρατό και του είχε δοθεί η ονομασία *φρυκτωρίες* (από τις λέξεις φρυκτός = πυρσός και ώρα = φροντίδα).

Σύμφωνα με την περιγραφή του έλληνα ιστορικού Πολύβιου, τον οπτικό τηλέγραφο επινόησαν - τελειοποίησαν οι αλεξανδρινοί τεχνικοί Κλεοξένης και Δημόκλειτος, που αποτέλεσε πραγματική επανάσταση στο χώρο των επικοινωνιών.

Αποτελούνταν από έναν πομπό και έναν δέκτη, που ο καθένας είχε από δύο τοίχους, που απείχαν μεταξύ τους λίγα μέτρα και ο σταθμός που έκανε τον δέκτη μπορούσε να τους διακρίνει άνετα με κάποια διόπτρα. Η εμβέλεια αυτού του τρόπου επικοινωνίας αποδείχθηκε στην πράξη ότι έφθανε μέχρι και τα 30 χιλιόμετρα.

Η κατασκευή των τοίχων θύμιζε πολεμίστρες, με έξι εσοχές και πέντε κοιλότητες. Η κάθε κοιλότητα φιλοξενούσε και από μία πυρσεία και είχε πλάτος περίπου ένα μέτρο. Όπως έβλεπε τον σταθμό εκπομπής ο δέκτης, ο αριστερός τοίχος αντιστοιχούσε στη σειρά των γραμμάτων και ο δεξιός στη στήλη των γραμμάτων.

Δηλαδή, είχαν χωρίσει τα γράμματα της αλφαβήτου σε πέντε ομάδες και σε πέντε στήλες, με την τελευταία σειρά και στήλη να έχουν από ένα γράμμα λιγότερο. Το κάθε γράμμα αντιστοιχούσε σε κάποια σειρά και κάποια στήλη και με κατάλληλα ανάμματα των πυρσών ο λήπτης λάμβανε τα γράμματα ένα-ένα. Κάθε ζευγάρι αριθμών αντιστοιχούσε και σε ένα γράμμα της αλφαβήτου.

Αν άναβαν δηλ. πρώτα δύο πυρσοί και μετά τρεις, σήμαινε τη δεύτερη στήλη και την τρίτη γραμμή, δηλ. την αποστολή του γράμματος κ.ο.κ. Με τον τρόπο αυτό γινόταν οι αποστολές όλων των γραμμάτων. Ο Πολύβιος αναφέρεται στην απλότητα και στην ακρίβεια που παρείχε αυτός ο κώδικας επικοινωνίας.

# Περιεχόμενα

# Πρόλογος

Η ψηφιακά κωδικοποιημένη πληροφορία κατά την διέλευσή της διά μέσου διαύλων επικοινωνίας με διαταραχές υφίσταται συχνά αλλοιώσεις. Το αντικείμενο της Θεωρίας των Κωδίκων Διορθωτών Λαθών είναι η κωδικοποίηση της πληροφορίας με τέτοιον τρόπο, ώστε αν μικρό πλήθος αλλοιώσεων έχει υπεισέλθει σ΄ ένα μήνυμα, η αποκωδικοποίησή του να τις διορθώνει. Σήμερα οι Κώδικες Διορθωτές Λαθών έχουν ευρεία εφαρμογή σε ηλεκτρονικούς υπολογιστές, σε σύμπακτους δίκτους, δορυφορικές επικοινωνίες, αποστολή φωτογραφιών από το διάστημα κλπ.

Η γέννηση της Θεωρίας των Κωδίκων Διορθωτών Λαθών ανάγεται στο περίφημο άρθρο του C. Shannon "A mathematical theory of communication" [17] το οποίο δημοσιεύτηκε στα 1948 και στο οποίο αποδεικνύεται η ύπαρξη αποτελεσματικών κωδίκων. Από τότε μέχρι σήμερα πολύ ερευνητική εργασία έχει γίνει με την χρήση τεχνικών από την Άλγεβρα, την Συνδυαστική και την Γεωμετρία για την κατασκευή κωδίκων που να διασφαλίζουν την αξιόπιστη διακίνηση της ψηφιακής πληροφορίας.

Το παρόν σύγγραμμα διαπραγματεύεται κυρίως τους αλγεβρικούς κώδικες, δηλαδή κώδικες που έχουν αλγεβρική δομή. Απευθύνεται σε φοιτητές τμημάτων Μαθηματικών, Πληροφορικής, Πολυτεχνικών Σχολών αλλά και σ΄ οποιονδήποτε ενδιαφέρεται για την κωδικοποίηση της πληροφορίας με σκοπό την προστασία της από διαταραχές που εμφανίζονται σε διαύλους επικοινωνίας. Απαραίτητες γνώσεις για την κατανόησή του είναι η βασική Άλγεβρα και Θεωρία Αριθμών.

Στην αρχή του συγγράματος παραθέτουμε μία ενότητα όπου υπενθυμίζουμε όλες τις έννοιες από την Άλγεβρα και Θεωρία Αριθμών που θα χρησιμοποιήσουμε. Στο πρώτο κεφάλαιο δίνουμε μία εισαγωγή στη κωδικοποίηση της πληροφορίας και στην αρχή που βασίζονται οι μέθοδοι διόρθωσή της. Στο δεύτερο κεφάλαιο περιγράφουμε την δομή των πεπερασμένων σωμάτων και μελετάμε τις βασικές ιδιότητες των γραμμι-

κών κωδίκων. Το τρίτο κεφάλαιο είναι αφιερωμένο σε μερικές βασικές ανισοτικές σχέσεις που συνδέουν τις παραμέτρους ενός κώδικα. Τρεις πολύ γνωστές οικογένειες γραμμικών κωδίκων με σημαντικές εφαρμογές, οι κώδικες του Hamming, οι κώδικες του Golay και οι κώδικες των Reed-Muller αποτελούν το αντικείμενο του τέταρτου κεφαλαίου. Στο πέμπτο κεφάλαιο μελετάμε μία από τις πλέον σημαντικές κατηγορίες γραμμικών κωδίκων, τους κυκλικούς κώδικες. Στο τελευταίο κεφάλαιο δίνουμε μερικές ακόμη ιδιότητες των πεπερασμένων σωμάτων τις οποίες χρησιμοποιούμε για την περιγραφή μίας πολύ ενδιαφέρουσας οικογένειας κυκλικών κωδίκων, τους κώδικες BCH, οι οποίοι έχουν ευρεία χρήση.

Τέλος, θα ήθελα να ευχαριστήσω τον μαθηματικό και υποψήφιο διδάκτορα του τμήματός μας Παρασκευά Αλβανό για την προσεκτική ανάγνωση των χειρογράφων και τις εποικοδομητικές παρατηρήσεις του.

Θεσσαλονίκη 2010 Δημήτριος Πουλάκης

# Συμβολισμοί - Ορολογία

Υποθέτουμε ότι ο αναγνώστης μας είναι εξοικειωμένος με την βασική Θεωρία Αριθμών και την βασική Άλγεβρα. Σ΄ αυτή την ενότητα υπενθυμίζουμε βασικούς ορισμούς, συμβολισμούς και αποτελέσματα από την Θεωρία Αριθμών και την Άλγεβρα. Για περισσότερες πληροφορίες σχετικά μ΄ αυτά ο αναγνώστης μπορεί να ανατρέξει στα [23], [4], [12], [21], [22].

Θα χρησιμοποιούμε τα συνήθη σύμβολα της Θεωρίας Συνολων: $\in$, $\subseteq$, $\subset$, $\emptyset$, $\cap$ και $\cup$. Αν $X$ και $Y$ είναι υποσύνολα του ίδιου συνόλου, τότε συμβολίζουμε με $X \setminus Y$ το σύνολο των στοιχείων του $X$ που δεν ανήκουν στο $Y$. Ένα σύνολο $X$ που έχει πεπερασμένο πλήθος στοιχείων καλείται πεπερασμένο και το πλήθος των στοιχείων του συμβολίζεται με $|X|$. Ας είναι $f : A \to B$ μία απεικόνιση. Η $f$ καλείται ένεση, αν για κάθε $x, y \in A$ με $x \neq y$ έχουμε $f(x) \neq f(y)$ και έφεση αν για κάθε $z \in B$ υπάρχει $x \in A$ με $f(x) = z$. Επίσης, η $f$ καλείται αμφίεση, αν είναι ένεση και έφεση. Θα συμβολίζουμε με $\mathbb{Z}$ το σύνολο των ακεραίων αριθμών και με $\mathbb{Q}$ και $\mathbb{R}$ τα σύνολα των ρητών και πραγματικών αριθμών, αντίστοιχα.

Ας είναι $E$ ένα μη κενό σύνολο. Ένα μη κενο σύνολο $\mathcal{R} \subseteq E \times E$ καλείται σχέση ισοδυναμίας επί του $E$, αν ισχύουν οι εξής ιδιότητες:
(α) $(a, a) \in \mathcal{R}$, για κάθε $a \in \mathcal{R}$.
(β) $(a, b) \in \mathcal{R}$ αν και μόνον αν $(b, a) \in \mathcal{R}$.
(γ) Αν $(a, b) \in \mathcal{R}$ και $(b, c) \in \mathcal{R}$, τότε $(a, c) \in \mathcal{R}$.
Σ΄ αυτή την περίπτωση συχνά γράφουμε $a \equiv b\ (\mathcal{R})$ αντί $(a, b) \in \mathcal{R}$. Τα σύνολα $[a] = \{x \in E/\ x \equiv a\ (\mathcal{R})\}$, $a \in E$, καλούνται κλάσεις ισοδυναμίας της $\mathcal{R}$. Το σύνολο των κλάσεων της $\mathcal{R}$ καλείται σύνολο πηλίκο του $E$ με την $\mathcal{R}$. Έχουμε $a \equiv b\ (\mathcal{R})$ αν και μόνον $[a] = [b]$. Το σύνολο των κλάσεων της $\mathcal{R}$ καλείται σύνολο πηλίκο της $\mathcal{R}$. Τα στοιχεία του αποτελούν μία διαμέριση του $E$, δηλαδή είναι μη κενά σύνολα, διαφορετικά ανά δύο και η ένωση τους δίνει το $E$. Αντίστροφα,

κάθε διαμέριση του $E$ ορίζει μία σχέση ισοδυναμίας επί αυτού.

Ας είναι $a$ και $b$ ακέραιοι. Τότε υπάρχουν μοναδικοί ακέραιοι $q$ και $r$ με $a = bq + r$ και $0 \leq r < |b|$. Αν $r = 0$, τότε λέμε ότι ο $a$ διαιρεί τον $b$ ή ότι ο $a$ είναι διαιρέτης του $b$ ή ακόμα ότι ο $b$ είναι πολλαπλάσιο του $a$ και γράφουμε $a|b$. Ας είναι $a_1, \ldots a_n$ ακέραιοι όχι όλοι μηδέν. Ο μεγαλύτερος από τους κοινούς θετικούς διαιρέτες τους καλείται μέγιστος κοινός διαιρέτης των $a_1, \ldots, a_n$ και συμβολίζεται με $\mu\kappa\delta(a_1, \ldots, a_n)$ και το μικρότερο από τα θετικά κοινά τους πολλαπλάσια καλείται ελάχιστο κοινό πολλαπλάσιο των $a_1, \ldots, a_n$ και συμβολίζεται με $\epsilon\kappa\pi(a_1, \ldots, a_n)$. Αν $\mu\kappa\delta(a_1, \ldots, a_n) = 1$, τότε οι ακέραιοι $a_1, \ldots, a_n$ καλούνται πρώτοι μεταξύ τους. Ένας θετικός ακέραιος $> 1$ που διαιρείται μόνο με το 1 και τον εαυτό του καλείται πρώτος. Σύμφωνα με το Θεμελιώδες Θεώρημα της Αριθμητικής κάθε θετικός ακέραιος $> 1$ γράφεται με μοναδικό τρόπο ως γινόμενο πρώτων αριθμών. Ας είναι $n$ ένας θετικός ακέραιος. Αν $a$ και $b$ είναι ακέραιοι, τότε γράφουμε $a \equiv b \pmod{n}$ και λέμε ότι οι $a$ και $b$ είναι ισότιμοι κατά μέτρο $n$ ή modulo $n$ αν και μόνον αν $n|a - b$. Η σχέση ισοτιμίας $\equiv$ είναι μία σχέση ισοδυναμίας στο $\mathbb{Z}$. Συμβολίζουμε με $\mathbb{Z}_n$ το σύνολο των κλασεων της. Αν $a$ είναι ακέραιος με $\mu\kappa\delta(a, n) = 1$, τότε καλούμε τάξη του $a$ modulo $n$ τον μικρότερο θετικό ακέραιο $r$ με $a^r \equiv 1 \pmod{n}$ και γράφουμε $\mathrm{ord}_n(a) = r$. Για κάθε ακέραιο $s$ με $a^s \equiv 1 \pmod{n}$ έχουμε $r|s$.

Ας είναι $G$ ένα μη κενό σύνολο εφοδιασμένο με μία πράξη $\star$, δηλαδή με μία απεικόνιση $\star : G \times G \to G$. Το ζεύγος $(G, \star)$ καλείται ομάδα αν ισχύουν τα εξής:
(α) $(a \star b) \star c = a \star (b \star c)$, για κάθε $a, b, c \in G$.
(β) Υπάρχει $e \in G$ τέτοιο, ώστε $a \star e = a = e \star a$, για κάθε $a \in G$.
(γ) Για κάθε $a \in G$ υπάρχει $a' \in G$ τέτοιο, ώστε $a \star a' = e = a' \star a$.
Αν επιπλέον ισχύει $a \star b = b \star a$, για κάθε $a, b \in G$, τότε η ομάδα $G$ καλείται αντιμεταθετική ή αβελιανή. Το $e$ καλείται ουδέτερο στοιχείο για την πράξη $\star$. Συχνά μία πράξη σ' ένα σύνολο $S$ συμβολίζεται ως πρόσθεση ή πολλαπλασιασμός. Τότε το ουδέτερο στοιχείο της παριστάνεται με $0_S$ ή $1_S$, αντίστοιχα.

Ας είναι $G$ μία ομάδα της οποίας η πράξη σημειώνεται ως πολλαπλασιασμός. Ένα μη κενό υποσύνολο $S$ της $G$ καλείται υποομάδα της $G$, αν το $S$ εφοδιασμένο με την ίδια πράξη είναι και αυτό ομάδα. Η ομάδα $G$ καλείται πεπερασμένη αν έχει πεπερασμένο πλήθος στοιχείων. Ας υποθέσουμε ότι η ομάδα $G$ είναι πεπερασμένη. Τότε ο ακέραιος $|G|$ καλείται τάξη της $G$. Αν υπάρχει $a \in G$ τέτοιο, ώστε $G = \{1_G, a, a^2, \ldots, a^{m-1}\}$, τότε η $G$ καλείται κυκλική και το $a$ γεννή-

τορας της. Για κάθε $a \in G$ καλούμε τάξη του $a$ τον μικρότερο θετικό ακέραιο $r$ με $a^r = 1_G$. Η τάξη του $a$ συμβολίζεται με $\mathrm{ord}(a)$. Σύμφωνα με το Θεώρημα του Langrange, για κάθε $a \in G$ η τάξη του $a$ διαιρεί την τάξη της $G$.

Ας είναι $(G, +)$ μία αβελιανή ομάδα και $H$ μία υποομάδα της. Τότε ορίζεται η εξής σχέση ισοδυναμίας επί της $G$:

$$a \sim b \iff a - b \in H.$$

Το σύνολο των κλάσεων της $\sim$ αποτελείται από τα σύνολα

$$a + H = \{a + b/\ b \in H\}, \quad a \in G$$

και συμβολίζεται με $G/H$. Το σύνολο $G/H$ με πράξη που ορίζεται από την σχέση $(a+H)+(b+H) = (a+b)+H$, για κάθε $a, b \in G$, δομείται σε αβελιανή ομάδα.

Ας είναι $G$, $H$ ομάδες και $f : G \to H$ μία απεικόνιση. Σημειώνουμε τις πράξεις των $G$ και $H$ με το σύμβολο του πολλαπλασιασμού. Η $f$ καλείται μορφισμός ομάδων, αν για κάθε $x, y \in G$ ισχύει $f(xy) = f(x)f(y)$. Αν ο μορφισμός $f$ είναι ένεση (αντίστοιχα έφεση), τότε καλείται μονομορφισμός (αντίστοιχα επιμορφισμός). Αν ο μορφισμός $f$ είναι ένεση και έφεση, τότε καλείται ισομορφισμός. Κάθε ισομορφισμός από το $G$ στο $G$ καλείται αυτομορφισμός. Το σύνολο $Ker(f) = f^{-1}(1_H)$ καλείται πυρήνας του $f$. Ο μορφισμός $f$ είναι ένεση αν και μόνον αν $Ker(f) = \{1_G\}$.

Ένα μη κενό σύνολο $A$ εφοδιασμένο με δύο πράξεις που σημειώνονται ως πρόσθεση και πολλαπλασιασμός καλείται δακτύλιος αν ισχύουν τα εξής:
(α) Το ζεύγος $(A, +)$ είναι αβελιανή ομάδα.
(β) Για κάθε $x, y, z \in A$ ισχύει $(xy)z = x(yz)$.
(γ) Υπάρχει στοιχείο $1_A \in A$ με $x1_A = x = 1_A x$, για κάθε $x \in A$.
(δ) Για κάθε $x, y, z \in A$ ισχύει

$$x(y + z) = xy + xz, \quad (x + y)z = xz + yz.$$

Αν για κάθε $x, y \in A$ ισχύει $xy = yx$, τότε ο δακτύλιος $A$ καλείται αντιμεταθετικός. Ένα στοιχείο $x \in A$ για το οποίο υπάρχει $x' \in A$ με $xx' = 1_A = x'x$ καλείται αντιστρέψιμο. Το σύνολο αυτών των στοιχείων αποτελεί ομάδα.

Ας υποθέσουμε τώρα ότι ο δακτύλιος $A$ είναι αντιμεταθετικός. Μία υποομάδα $I$ του $A$ καλείται ιδεώδες του $A$, αν για κάθε $a \in A$ και $x \in I$

έχουμε $ax \in I$. Για κάθε $a \in A$ το σύνολο $(a) = \{xa/\ x \in A\}$ είναι ένα ιδεώδες του $A$. Ένα μη κενό υποσύνολο του $A$ που είναι και αυτό δακτύλιος με τις ίδιες πράξεις μ΄ αυτές του $A$ καλείται υποδακτύλιος του $A$. Αν $I$ είναι ένα ιδεώδες του δακτυλίου $A$, τότε η αβελιανή ομάδα $A/I$ δομείται σε δακτύλιο με πολλαπλασιασμό που ορίζεται από την σχέση $(a+I)(b+I) = (ab)+I$, για κάθε $a, b \in A$.

Ένας μορφισμός από τον δακτύλιο $A$ στον $B$ είναι μία απεικόνιση $f : A \to B$ τέτοια, ώστε για κάθε $a, b \in A$ έχουμε

$$f(a+b) = f(a) + f(b), \quad f(ab) = f(a)f(b), \quad f(1_A) = 1_B.$$

Αν επιπλέον ο μορφισμός $f$ είναι ένεση (αντίστοιχα έφεση), τότε ο μορφισμός $f$ καλείται μονομορφισμός (αντίστοιχα επιμορφισμός). Αν ο μορφισμός $f$ είναι συγχρόνως ένεση και έφεση, τότε καλείται ισομορφισμός. Στη περίπτωση όπου ο $f$ είναι ισομορφισμός, λέμε ότι οι δακτύλιοι $A$ και $B$ είναι ισόμορφοι και γράφουμε $A \cong B$. Ένας ισομορφισμός από τον δακτύλιο $A$ στον εαυτό του καλείται αυτομορφισμός. Το σύνολο $Ker(f) = f^{-1}(0_B)$ καλείται πυρήνας του $f$ και είναι ιδεώδες του $A$. Έχουμε $Ker(f) = \{0_A\}$, αν και μόνον αν η $f$ είναι ένεση. Επίσης, η εικόνα $f(A)$ του $f$ είναι υποδακτύλιος του $B$ και ισχύει $A/Ker(f) \cong f(A)$.

Ο δακτύλιος $A$ καλείται σώμα αν κάθε μη μηδενικό του στοιχείο είναι αντιστρέψιμο. Ο δακτύλιος $\mathbb{Z}_n$ είναι σώμα αν και μόνον αν ο ακέραιος $n$ είναι πρώτος. Στη περίπτωση όπου $p$ είναι πρώτος, συχνά γράφουμε $\mathbb{F}_p$ αντί $\mathbb{Z}_p$. Ας είναι $K$ σώμα. Θεωρούμε την ακολουθία $1_K, 2 \cdot 1_K, 3 \cdot 1_K, \ldots$ . Αν κανένας από τους όρους της παραπάνω ακολουθίας δεν είναι το μηδέν, τότε λέμε ότι το $K$ έχει χαρακτηριστική 0. Αν κάποιος από τους όρους της ακολουθίας είναι το μηδενικό στοιχείο, τότε χαρακτηριστική του $K$ καλείται ο μικρότερος ακέραιος $n > 0$ για τον οποίο ισχύει $n1_K = 0$. Σ΄ αυτή την περίπτωση ο $n$ είναι πρώτος. Η χαρακτηριστική του $A$ συμβολίζεται με $char(A)$. Αν $char(K) = 0$, τότε υπάρχει ένας μονομορφισμός $\sigma : \mathbb{Q} \to K$ και αν $char(A) = p > 0$, ένας μονομορφισμός $\tau : \mathbb{F}_p \to K$.

Καλούμε $m \times n$ πίνακα με στοιχεία από το σώμα $K$ ένα ορθογώνιο σχήμα με $m$ γραμμές και $n$ στήλες

$$A = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{m1} & a_{m2} & \ldots & a_{mn} \end{pmatrix},$$

που σχηματίζονται από $mn$ στοιχεία $a_{ij} \in K$ $(i = 1, \ldots, m,\ j = 1, \ldots, n)$. Ο $1 \times n$ πίνακας $(a_{i1} \ldots a_{in})$ καλείται $i$-οστή γραμμή του $A$ και ο $m \times 1$-πίνακας

$$\begin{pmatrix} a_{1j} \\ \vdots \\ a_{mj} \end{pmatrix}$$

$j$-οστή στήλη του $A$. Το στοιχείο $a_{ij}$ που βρίσκεται στη διασταύρωση της $i$-γραμμής και της $j$-στήλης καλείται $(i, j)$-*στοιχείο* του πίνακα $A$. Συχνά θα γράφουμε για συντομία $A = (a_{ij})_{m\times n}$ ή $A = (a_{ij})$. Συμβολίζουμε με $M_{m\times n}(K)$ το σύνολο των $m \times n$-πινάκων με στοιχεία από το $K$. Καλούμε ανάστροφο του πίνακα $A$ τον πίνακα ${}^tA$ που προκύπτει από τον $A$, αν οι γραμμές του $A$ γίνουν στήλες και οι στήλες γραμμές.

Καλούμε τους πίνακες $A = (a_{ij})$ και $B = (b_{ij})$ του $M_{m\times n}(K)$ *ίσους*, και γράφουμε $A = B$, αν ισχύει $a_{ij} = b_{ij}$, για κάθε $i = 1, \ldots, m$ και $j = 1, \ldots, n$. Αν $A = (a_{ij})$ και $B = (b_{ij})$ είναι δύο πίνακες του $M_{m\times n}(K)$, τότε ορίζουμε ως άθροισμα των $A$ και $B$ τον πίνακα $A+B = (a_{ij} + b_{ij})$. Αν $A = (a_{ij}) \in M_{m\times n}(K)$ και $B = (b_{ij}) \in M_{n\times k}(K)$, τότε ορίζουμε ως γινόμενο των $A$ και $B$ τον πίνακα $AB = (c_{ik})$ του $M_{m\times k}(K)$, όπου $c_{ik} = a_{i1}b_{1k} + \cdots + a_{in}b_{nk}$. Το σύνολο $M_{m\times m}(K)$ εφοδιασμένο μ΄ αυτές τις πράξεις δομείται σε δακτύλιο. Το ουδέτερο στοιχείο για την πρόσθεση είναι ο πίνακας $O$ που σε όλες τις θέσεις του έχει το 0 και καλείται μηδενικός. Το ουδέτερο στοιχείο για τον πολλαπλασιασμό είναι ο πίνακας

$$I_m = \begin{pmatrix} 1 & 0 & \ldots & 0 \\ 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 \end{pmatrix}$$

που καλείται μοναδιαίος.

Ας είναι $K$ ένα σώμα. Ένα πολυώνυμο ως προς την απροσδιόριστη $X$ επί του $K$ είναι μία τυπική έκφραση της μορφής $f(X) = a_0 + a_1X + \cdots + a_kX^k$, όπου $a_0, \ldots, a_k \in K$. Τα στοιχεία $a_0, \ldots, a_k$ καλούνται συντελεστές του $f(X)$. Αν $f(X) \neq 0$, τότε καλούμε βαθμό του $f(X)$, και τον συμβολίζουμε με $\deg f(X)$, τον μεγαλύτερο φυσικό $n$ έτσι, ώστε $a_n \neq 0$. Επίσης, θέτουμε $\deg 0 = -\infty$. Το πολυώνυμο $f(X)$ καλείται κανονικό, αν ο συντελεστής της μεγαλύτερης δύναμης του $X$ είναι 1. Το σύνολο των πολυωνύμων ως προς $X$ επί του $K$ συμβολίζεται

με $K[X]$. Ας είναι $f(X) = a_0 + \cdots + a_m X^m$ και $g(X) = b_0 + \cdots + b_n X^n$ δύο πολυώνυμα του $K[X]$. Τότε $f(X) = g(X)$, αν και μόνον αν $n = m$ και $a_i = b_i$ $(i = 0, \ldots, m)$. Το άθροισμα και το γινόμενο των $f(X)$ και $g(X)$ είναι

$$(f+g)(X) = \sum_{i=0}^{\max\{m,n\}} (a_i + b_i)X^i, \quad (fg)(X) = \sum_{i=0}^{m+n} (\sum_{k+l=i} a_k b_l)X^i,$$

αντίστοιχα. Το σύνολο $K[X]$ εφοδιασμένο με τις δύο αυτές πράξεις αποτελεί αντιμεταθετικό δακτύλιο.

Ας είναι $f(X)$ και $g(X)$ δύο πολυώνυμα του $K[X] \setminus \{0\}$. Τότε υπάρχουν $q(X), r(X) \in K[X]$ έτσι, ώστε $f(X) = g(X)q(X) + r(X)$ και $\deg r(X) < \deg g(X)$. Αν $r(X) = 0$, τότε λέμε ότι το $g(X)$ διαιρεί το $f(X)$ ή ότι το $f(X)$ είναι πολλαπλάσιο του $g(X)$ και γράφουμε $g(X)|f(X)$. Ας είναι $f_1(X), \ldots, f_n(X) \in K[X]$. Ένα κανονικό πολυώνυμο $D(X) \in K[X]$ καλείται μέγιστος κοινός διαιρέτης των $f_1(X), \ldots, f_n(X)$ και συμβολίζεται με $\mu\kappa\delta(f_1(X), \ldots, f_n(X))$, αν ισχύουν τα εξής:
(α) $D(X)|f_i(X)$ $(i = 1, \ldots, n)$.
(β) Αν $\Delta(X) \in K[X]$ και $\Delta(X)|f_i(X)$ $(i = 1, \ldots, n)$, τότε έχουμε $\Delta(X)|D(X)$.
Αν $\mu\kappa\delta(f_1(X), \ldots, f_n(X)) = 1$, τότε λέμε ότι τα $f_1(X), \ldots, f_n(X)$ είναι πρώτα μεταξύ τους. Σ′ αυτή την περίπτωση υπάρχουν πολυώνυμα $a_1(X), \ldots, a_n(X) \in K[X]$ τέτοια, ώστε

$$a_1(X)f_1(X) + \cdots + a_n(X)f_n(X) = 1.$$

Ένα πολυώνυμο $f \in K[X]$ καλείται ανάγωγο στο $K[X]$, αν δεν υπάρχουν πολυώνυμα $g_1(X), g_2(X) \in K[X]$ με $f(X) = g_1(X)g_2(X)$ και $0 < \deg g_i(X) < \deg f(X)$ $(i = 1, 2)$.

Αν $f(X) = \sum_{i=0}^{n} a_i X^i$ είναι πολυώνυμο του $K[X]$ και $x \in K$, τότε το στοιχείο $f(x) = \sum_{i=0}^{n} a_i x^i$ καλείται τιμή του $f$ στο $x$. Ένα στοιχείο $a \in K$ καλείται ρίζα του $f(X)$ πολλαπλότητας $k > 0$, αν υπάρχει $q(X) \in K[X]$ με $q(a) \neq 0$ έτσι, ώστε $f(X) = (X - a)^k q(X)$. Καλούμε τυπική παράγωγο ή απλώς παράγωγο του $f(X)$ το πολυώνυμο

$$f'(X) = a_1 + 2a_2 X + \cdots + n a_n X^{n-1}.$$

Η ρίζα $a$ του $f(X)$ έχει πολλαπλότητα $> 1$ αν και μόνον αν $f'(a) = 0$.

Ας είναι $K$ ένα σώμα. Καλούμε γραμμικό ή διανυσματικό χώρο επί του $K$ κάθε μη κενό σύνολο $V$ εφοδιασμένο με μία πρόσθεση $V \times V \to V,\ (x,y) \mapsto x+y$ και ένα βαθμωτό πολλαπλασιασμό $K \times V \to V,\ (k,x) \mapsto kx$ που έχουν τις εξής ιδιότητες:
(α) Το ζεύγος $(V,+)$ αποτελεί αβελιανή ομάδα.
(β) Για κάθε $x,y \in V$ και $a,b \in K$ ισχύουν τα παρακάτω:

1. $a(x+y) = ax + ay$,
2. $(a+b)x = ax + bx$,
3. $a(bx) = (ab)x$,
4. $1x = x$.

Τα στοιχεία του $V$ καλούνται διανύσματα. Ένα μη κενό υποσύνολο $W$ του $V$ καλείται γραμμικός ή διανυσματικός υποχώρος του $V$ αν για κάθε $u,v \in W$ και $k,l \in K$ έχουμε $ku + lv \in W$.

Ας είναι $v_1,\ldots,v_k \in V$. Συμβολίζουμε με $< v_1,\ldots,v_k >$ το σύνολο που αποτελείται από όλα τα στοιχεία της μορφής $a_1v_1 + \cdots + a_kv_k$, όπου $a_1,\ldots,a_k \in K$. Το σύνολο αυτό είναι γραμμικός υποχώρος του $V$ και καλείται γραμμικός υποχώρος παραγόμενος από τα $v_1,\ldots,v_k$. Το σύνολο $\{v_1,\ldots,v_k\}$ καλείται γραμμικά ανεξάρτητο, αν δεν υπάρχουν $a_1,\ldots,a_k \in K$ όχι όλα μηδέν με $a_1v_1 + \cdots + a_kv_k = 0$. Το σύνολο $\{v_1,\ldots,v_k\}$ καλείται βάση του $V$, αν είναι γραμμικά ανεξάρτητο και $< v_1,\ldots,v_k >= V$. Αν ο γραμμικός χώρος $V$ παράγεται από ένα πεπερασμένο πλήθος στοιχείων, τότε όλες οι βάσεις του $V$ έχουν το ίδιο πεπερασμένο πλήθος στοιχείων που καλείται διάσταση του $V$ και συμβολίζεται με $\dim V$. Αν $W$ είναι ένας γραμμικός υποχώρος του $V$, τότε η αβελιανή ομάδα $V/W$ δομείται σε γραμμικό χώρο με βαθμωτό πολλαπλασιασμό που ορίζεται από την σχέση $a(x+W) = (ax)+W$, για κάθε $a \in K$ και $x \in V$.

Ας είναι $V$, $W$ δύο γραμμικοί χώροι επί του σώματος $K$. Μία απεικόνιση $f : V \to W$ καλείται γραμμική, αν για κάθε $x,y \in V$ έχουμε $f(x+y) = f(x) + f(y)$ και για κάθε $a \in K$ και $x \in V$ έχουμε $f(ax) = af(x)$. Αν η γραμμική απεικόνιση $f$ είναι ένεση (αντίστοιχα έφεση), τότε καλείται μονομορφισμός (αντίστοιχα επιμορφισμός). Αν η γραμμική απεικόνιση $f$ είναι συγχρόνως ένεση και έφεση, τότε καλείται ισομορφισμός. Στη περίπτωση όπου η $f$ είναι ισομορφισμός, λέμε ότι οι γραμμικοί χώροι $V$ και $W$ είναι ισόμορφοι και γράφουμε $V \cong W$. Το σύνολο $Ker(f) = f^{-1}(0)$ καλείται πυρήνας της $f$ και

είναι γραμμικός υποχώρος του $V$. Επίσης, ισχύει $V/Ker(f) \cong f(V)$. Η γραμμική απεικόνιση $f$ είναι ένεση αν και μόνον αν $Ker(f) = \{0\}$. Αν $V$ είναι γραμμικός χώρος με $\dim V = n$, τότε ισχύει η εξίσωση $\dim V = \dim Ker(f) + \dim f(V)$. Επιπλέον, έχουμε $V \cong K^n$.

Ας είναι $M$ ένας πίνακας με στοιχεία από το σώμα $K$. Το πλήθος των γραμμικά ανεξαρτήτων γραμμών του $M$ ισούται με το πλήθος των γραμμικά ανεξαρτήτων στηλών του και καλείται βαθμίδα του $M$.

# Κεφάλαιο 1

# Κωδικοποίηση

Σ΄ αυτό το κεφάλαιο γίνεται μία εισαγωγή στη κωδικοποίηση της πληροφορίας και στον τρόπο με τον οποίο επιτυγχάνεται η διόρθωση των λαθών κατά την μετάδοσή της.

## 1.1 Εισαγωγή

Η ανάπτυξη των μεθόδων και μέσων επικοινωνίας δημιούργησε την ανάγκη της *κωδικοποίησης* της πληροφορίας, δηλαδή, την παράστασή της με ακολουθίες απλών και εύχρηστων συμβόλων, κατάλληλων για την επιτυχή διέλευσή της από τους επιθυμητούς διαύλους. Σε πολλές περιπτώσεις οι δίαυλοι επικοινωνίας υφίστανται πολλές διαταραχές, οι οποίες έχουν ως αποτέλεσμα την αλλοίωση της διερχόμενης πληροφορίας. Ένα τέτοιο παράδειγμα είναι η αποστολή πληροφοριών από διαστημόπλοια ή δορυφόρους. Έτσι, ιδιαίτερη σημασία έχει δοθεί στην ανάπτυξη μεθόδων κωδικοποίησης τέτοιων, ώστε η *αποκωδικοποίηση* της πληροφορίας, δηλαδή η επανάκτησή της μετά την διέλευσή της από τον επιθυμητό δίαυλο, να διορθώνει τα λάθη τα οποία εισχώρησαν σ΄ αυτήν.

Ένα πεπερασμένο σύνολο $A$ του οποίου τα στοιχεία χρησιμοποιούνται για την κωδικοποίηση δεδομένων καλείται *αλφάβητο* και τα στοιχεία του *γράμματα*. Ένα κλασσικό παράδειγμα τέτοιου αλφαβήτου είναι το σύνολο $B = \{0, 1\}$. Για κάθε θετικό ακέραιο $n$ τα στοιχεία του συνόλου $A^n$ καλούνται *λέξεις μήκους* $n$. Συχνά στις εφαρμογές οι λέξεις $(a_1, \ldots, a_n)$ του $A^n$ συμβολίζονται με $a_1 \cdots a_n$. Ας δούμε στη συνέχεια μερικά παραδείγματα κωδικοποιήσεων.

**Παράδειγμα 1.1** *Κώδικας του Morse.* Για την μετάδοση των γραμμάτων του αγγλικού αλφαβήτου δια μέσου του τηλέγραφου, ο οποίος εφευρέθηκε στα 1838, ο Morse πρότεινε την κωδικοποίηση τους μ΄ ένα αλφάβητο που αποτελείται από τρία στοιχεία: την τελεία, την παύλα και το κενό διάστημα. Για την παράσταση ενός γράμματος χρησιμοποιούνται τελείες και παύλες που χωρίζονται από ένα κενό διάστημα. Δύο γράμματα χωρίζονται από τρία κενά διαστήματα και δύο λέξεις από έξι κενά διαστήματα. Οι λέξεις του κώδικα του Morse δίνονται στον παρακάτω πίνακα.

**ΠΙΝΑΚΑΣ 1**
**Κώδικας του Morse**

| | | | |
|---|---|---|---|
| $A$ | $\cdot\ -$ | $N$ | $-\ \cdot$ |
| $B$ | $-\ \cdot\ \cdot\ \cdot$ | $O$ | $-\ -\ -$ |
| $C$ | $-\ \cdot\ -\ \cdot$ | $P$ | $\cdot\ -\ -\ \cdot$ |
| $D$ | $-\ \cdot\ \cdot$ | $Q$ | $-\ -\ \cdot\ -$ |
| $E$ | $\cdot$ | $R$ | $\cdot\ -\ \cdot$ |
| $F$ | $\cdot\ \cdot\ -\ \cdot$ | $S$ | $\cdot\ \cdot\ \cdot$ |
| $G$ | $-\ -\ \cdot$ | $T$ | $-$ |
| $H$ | $\cdot\ \cdot\ \cdot\ \cdot$ | $U$ | $\cdot\ \cdot\ -$ |
| $I$ | $\cdot\ \cdot$ | $V$ | $\cdot\ \cdot\ \cdot\ -$ |
| $J$ | $\cdot\ -\ -\ -$ | $W$ | $\cdot\ -\ -$ |
| $K$ | $-\ \cdot\ -$ | $X$ | $-\ \cdot\ \cdot\ -$ |
| $L$ | $\cdot\ -\ \cdot\ \cdot$ | $Y$ | $-\ \cdot\ -\ -$ |
| $M$ | $-\ -$ | $Z$ | $-\ -\ \cdot\ \cdot$ |

Παρατηρούμε ότι τα γράμματα που εμφανίζονται συχνά, όπως το $E$, κωδικοποιούνται με λίγα σύμβολα. Αντιστρόφως, γράμματα που εμφανίζονται λιγότερο συχνά, όπως το $Z$, κωδικοποιούνται με τέσσερα σύμβολα.

Ας σημειωθεί ότι διαταραχές στο δίαυλο επικοινωνίας είναι δυνατόν να προκαλέσουν αλλοίωση των γραμμάτων του αποστελλόμενου μηνύματος με συνέπεια πολλές φορές να αλλοιώνεται το νόημά του. Για παράδειγμα, ας υποθέσουμε ότι η Alice στέλνει στον Jim το εξής μήνυμα:

*"Send the car to John"*

Αν κατά την αποστολή του μηνύματος το $r$ της λέξης *car* μεταβληθεί σε $t$, τότε ο Jim λαμβάνει το εξής μήνυμα:

*"Send the cat to John"*

Αν αυτό το μήνυμα έχει κάποια σημασία για τον Jim , τότε η αλλοίωση ενός και μόνο γράμματος είχε ως συνέπεια την ουσιαστική αλλοίωση του μηνύματος. Ο κώδικας του Morse δεν προσφέρει κανένα τρόπο προφύλαξης από τέτοια λάθη μετάδοσης.

**Παράδειγμα 1.2** *Κώδικας ISBN (International Standard Book Number).* Αυτό είναι ένα διεθνές σύστημα ταξινόμησης των βιβλίων που εκδίδονται σήμερα. Κάθε βιβλίο χαρακτηρίζεται μοναδικά από δέκα αριθμούς $x_1, \ldots, x_{10}$. Οι $x_1, \ldots, x_9$ ανήκουν στο σύνολο $\{0, \ldots, 9\}$. Ο $x_1$ δηλώνει την γλώσσα στην οποία είναι γραμμένο το βιβλίο, ο $x_2x_3$ τον εκδότη του βιβλίου και ο $x_4x_5x_6x_7x_8x_9$ είναι ο αριθμός που δίνεται στο βιβλίο από τον εκδότη. Ο $x_{10}$ είναι ένας ακέραιος με $0 \leq x_{10} \leq 10$ τέτοιος, ώστε

$$\sum_{i=1}^{10} ix_i \equiv 0 \pmod{11},$$

ή ισοδύναμα

$$x_{10} \equiv \sum_{i=1}^{9} ix_i \pmod{11}.$$

Αν $x_{10} = 10$, τότε στη θέση του $x_{10}$ τίθεται το σύμβολο $X$. Για παράδειγμα το βιβλίο του Δ. Πουλάκη *Θεωρία Αριθμών* που έχει εκδοθεί από τις Εκδόσεις Ζήτη έχει ISBN $9-60-431429-7$, ενώ το βιβλίο της Judy L. Walker *Codes and Curves* που έχει εκδοθεί από την Αμερικάνικη Μαθηματική Εταιρεία έχει ISBN $0-82-182628-X$. Συνεπώς, το χρησιμοποιούμενο αλφάβητο είναι το σύνολο $\{0, \ldots, 9, X\}$.

Ας υποθέσουμε τώρα ότι $x_1 - x_2x_3 - x_4x_5x_6x_7x_8x_9 - x_{10}$ είναι ο ISBN ενός βιβλίου και ότι κατά την μετάδοσή του δια μέσου ενός διαύλου επικοινωνίας αλλοιώνεται μόνο το ψηφίο $x_j$. Τότε ο παραλήπτης λαμβάνει τον αριθμό $y_1 - y_2y_3 - y_4y_5y_6y_7y_8y_9 - y_{10}$, όπου $y_i = x_i$ για $i \neq j$ και $y_j = x_j + a$ με $a \neq 0$. Καθώς

$$\sum_{i=1}^{10} iy_i \equiv \left(\sum_{i=1}^{10} ix_i\right) + ja \equiv ja \not\equiv 0 \pmod{11},$$

ο παραλήπτης βλέπει ότι ο παραπάνω αριθμός δεν αντιστοιχεί σε κανένα βιβλίο. Επίσης, αν το $x_j$ έχει αλλάξει θέση με το $x_k$ και $x_j \neq x_k$, τότε

ο παραλήπτης λαμβάνει τον αριθμό $y_1 - y_2y_3 - y_4y_5y_6y_7y_8y_9 - y_{10}$, όπου $y_i = x_i$ για $i \neq j, k$ και $y_j = x_k$, $y_k = x_j$. Επομένως, έχουμε

$$\sum_{i=1}^{10} iy_i \equiv \sum_{i=1}^{10} ix_i + (k-j)x_j + (j-k)x_k \equiv (k-j)(x_j - x_k) \not\equiv 0 \pmod{11}$$

και κατά συνέπεια ο παραπάνω αριθμός δεν αντιστοιχεί σε κανένα βιβλίο.

Βλέπουμε, λοιπόν, ότι ο κώδικας ISBN έχει την ικανότητα να ανιχνεύει την παρουσία λαθών της παραπάνω μορφής. Δεν έχει όμως την ικανότητα να εντοπίσει την θέση τους και κατά συνέπεια να τα διορθώσει. Σ΄ αυτή την περίπτωση ζητείται, εάν είναι δυνατόν, η επαναμετάδοση της αλλοιωμένης λέξης του ISBN.

**Παράδειγμα 1.3** *Κώδικας ASCII (American Standard Code for Information Interchange).* Η ανάγκη της παράστασης της πληροφορίας στο εσωτερικό των αριθμομηχανών και κατόπιν των ηλεκτρονικών υπολογιστών οδήγησε στη χρήση κωδίκων. Καθώς οι ηλεκτρονικοί υπολογιστές διαχειρίζονται μόνο δύο καταστάσεις που χαρακτηρίζονται συμβολικά από τα 0 και 1, κάθε πληροφορία που δίνεται σ΄ αυτούς παριστάνεται από μία λέξη του αλφαβήτου $B = \{0, 1\}$.

Ένας ευρέως χρησιμοποιούμενος κώδικας που αντιστοιχεί τα γράμματα του λατινικού αλφαβήτου (μικρά και κεφαλαία), τους αριθμούς, τα σημεία στίξης και άλλα σύμβολα σε οκτάδες από 0 και 1 είναι ο κώδικας ASCII. Όλες οι επτάδες που αποτελούνται από 0 και 1 είναι αρκετές για την κωδικοποίηση των παραπάνω συμβόλων. Καθώς όμως είναι πρακτικά αδύνατη η αποφυγή λαθών στο εσωτερικό ενός υπολογιστή, κάθε στοιχείο του κώδικα ASCII έχει προκύψει από την παράθεση στο τέλος κάθε λέξης του $B^7$ ενός ογδόου συμβόλου που είναι 0 ή 1 έτσι, ώστε το συνολικό πλήθος των 1 στο εν λόγω στοιχείο να είναι άρτιο. Για παράδειγμα, οι λέξεις 1000110 και 1000111 έχουν τρία και τέσσερα 1, αντιστοιχα. Οπότε, στο τέλος τους παραθέτουμε το 1 και το 0, αντίστοιχα, και έτσι προκύπτουν οι λέξεις του κώδικα ASCII 10001101 και 10001111.

Στην περίπτωση όπου ένα μόνο λάθος υπεισέλθει σε μία λέξη του κώδικα ASCII, η ύπαρξή του γίνεται αμέσως αντιληπτή. Πράγματι, αν μόνο ένα από τα σύμβολα μίας λέξης $x$ αλλοιωθεί και προκύψει η λέξη $y$, τότε το πλήθος των 1 στην $y$ θα είναι περιττό και επομένως η $y$ δεν θα είναι λέξη του ASCII. Από την άλλη πλευρά όμως, ο ASCII δεν έχει την ικανότητα εντοπισμού του λάθους και επομένως της διόρθωσής του. Έτσι, σ΄ αυτή την περίπτωση ζητείται η επαναμετάδοση της λέξης.

Στον παρακάτω πίνακα παρατίθενται τα γράμματα του λατινικού αλφαβήτου και οι αντίστοιχες λέξεις του κώδικα ASCII.

**ΠΙΝΑΚΑΣ 2**
**Αντιστοιχία λατινικού αλφαβήτου με λέξεις του ASCII.**

| | | | |
|---|---|---|---|
| $A$ | 10000010 | $N$ | 10011100 |
| $B$ | 10000100 | $O$ | 10011111 |
| $C$ | 10000111 | $P$ | 10100000 |
| $D$ | 10001000 | $Q$ | 10100011 |
| $E$ | 10001011 | $R$ | 10100101 |
| $F$ | 10001101 | $S$ | 10100110 |
| $G$ | 10001110 | $T$ | 10101001 |
| $H$ | 10010000 | $U$ | 10101010 |
| $I$ | 10010011 | $V$ | 10101100 |
| $J$ | 10010101 | $W$ | 10101111 |
| $K$ | 10010110 | $X$ | 10110001 |
| $L$ | 10011001 | $Y$ | 10110010 |
| $M$ | 10011010 | $Z$ | 10110100 |

**Παράδειγμα 1.4** *Τριπλός κώδικας ελέγχου.* Ας υποθέσουμε οτι επιθυμούμε να μεταδόσουμε μία πληροφορία που έχει κωδικοποιηθεί με το αλφάβητο $B$ (για παράδειγμα με την χρήση του κώδικα ASCII). Για την ασφαλέστερη μετάδοσή της εφαρμόζουμε επιπλέον την εξής κωδικοποίηση: Χωρίζουμε την ακολουθία των 0 και 1 σε τμήματα που αποτελούνται από τρία ψηφία. Ας είναι $abc$ ένα τέτοιο τμήμα. Τότε επισυνάπτουμε σ΄ αυτό τα ψηφία $x, y, z \in B$ που είναι τέτοια, ώστε

1. το πλήθος των 1 στη λέξη $abx$ να είναι άρτιο,
2. το πλήθος των 1 στη λέξη $acy$ να είναι άρτιο,
3. το πλήθος των 1 στη λέξη $bcz$ να είναι άρτιο.

Για παράδειγμα, αν $abc = 100$, τότε $x = 1$, $y = 1$ και $z = 0$. Δηλαδή, $abcxyz = 100110$.

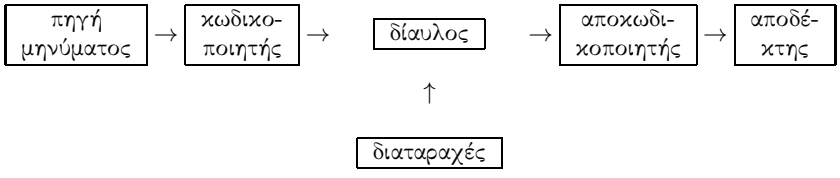
Στην περίπτωση όπου κατά την μετάδοση της λέξης $abcxyz$ αλλοιωθεί μόνο ένα γράμμα της, τότε παρατηρούμε τα εξής: Το $a$ είναι αλλοιωμένο αν και μόνον αν οι προτάσεις (1) και (2) δεν ισχύουν, το $b$ είναι αλλοιωμένο αν και μόνον αν οι (1) και (3) δεν ισχύουν και το $c$ είναι αλλοιωμένο, αν και μόνον αν οι (2) και (3) δεν ισχύουν. Επίσης,

το $x$ έχει αλλοιωθεί αν και μόνον αν η (1) δεν ισχύει, το $y$ έχει αλλοιωθεί αν και μόνον αν η (2) δεν ισχύει και το $z$ έχει αλλοιωθεί αν και μόνον αν η (3) δεν ισχύει. Έτσι, αν ένα μόνο γράμμα της λέξης $abcxyz$ αλλοιωθεί, τότε αυτό γίνεται αντιληπτό. Επιπλέον, είναι δυνατόν να το διορθώσουμε με τον εξής τρόπο: Αν οι (1) και (2) δεν ισχύουν, τότε διορθώνουμε το $a$, αν οι (1) και (3) δεν ισχύουν, τότε διορθώνουμε το $b$ και αν οι (2) και (3) δεν ισχύουν, τότε διορθώνουμε το $c$. Επίσης, αν μόνον μία από τις (1), (2), (3) δεν ισχύει, τότε αντίστοιχα διορθώνουμε το $x$, $y$ ή $z$.

Ας δούμε τώρα τι συμβαίνει στην περίπτωση όπου δύο το πολύ σύμβολα της $abcxyz$ έχουν αλλοιωθεί. Αν τα $a$ και $b$ έχουν αλλοιωθεί, τότε οι (2) και (3) δεν ισχύουν. Σ′ αυτή την περίπτωση η (1) ισχύει. Επίσης, αν τα $y$ και $z$ έχουν αλλοιωθεί, τότε οι (2) και (3) δεν ισχύουν. Τέλος, αν μόνο το $c$ έχει αλλοιωθεί, τότε οι (2) και (3) δεν ισχύουν. Έτσι, αν γνωρίζουμε ότι το πολύ δύο σύμβολα έχουν αλλοιωθεί και δούμε ότι οι (2) και (3) δεν ισχύουν, δεν μπορούμε να είμαστε βέβαιοι αν έχουν αλλοιωθεί τα $a$, $b$ ή τα $x$, $y$ ή το $c$. Σε αντίστοιχα συμπεράσματα καταλήγουμε αν θεωρήσουμε και τα υπόλοιπα ζεύγη συμβόλων της λέξης $abcxyz$.

Συνοψίζοντας, είδαμε ότι η κωδικοποίηση με τον κώδικα του Morse δεν μας εξασφαλίζει την ανίχνευση λάθους, η κωδικοποίηση με τους κώδικες ISBN και ASCII , στην περίπτωση μόνο ενός λάθους, ανιχνεύει την παρουσία του (όχι όμως και την θέση του), ενώ ο τριπλός κώδικας ελέγχου όχι μόνο ανιχνεύει την παρουσία λάθους, όταν υπάρχει μόνο ένα, αλλά μας δίνει και την θέση του με συνέπεια την διόρθωσή του.

Σκοπός αυτού του κεφαλαίου και των επομένων είναι η εισαγωγή του αναγνώστη σε μεθόδους κωδικοποίησης της πληροφορίας οι οποίες δίνουν την δυνατότητα διόρθωσης λαθών που εμφανίζονται σε μηνύματα που μεταδίδονται δια μέσου διαύλων επικοινωνίας οι οποίοι παρουσιάζουν διαταραχές. Τέτοιοι δίαυλοι είναι οι ραδιοεπικοινωνίες παντός είδους, τα δορυφορικά επικοινωνιακά συστήματα, τα πληροφοριακά συστήματα κλπ. Ένα γενικό μοντέλο συστήματος επικοινωνίας δίνεται στο παρακάτω σχήμα.



Η διέλευση της πληροφορίας σ΄ ένα τέτοιο σύστημα γίνεται είτε με διακριτό τρόπο π.χ. οι κουκίδες μίας τηλεοπτικής εικόνας, είτε με συνεχή π.χ. η μουσική στο ράδιο. Θ΄ ασχοληθούμε μόνο με διαύλους στους οποίους η πληροφορία διέρχεται με διακριτό τρόπο, κωδικοποιημένη με την βοήθεια ενός αλφαβήτου $A$, και οι οποίοι έχουν τις εξής δύο ιδιότητες:

1. Κάθε σύμβολο του $A$ έχει την ίδια πιθανότητα αλλοίωσης κατά την μετάδοση που είναι $p < 1/2$.

2. Εάν ένα σύμβολο του $A$ αλλοιωθεί, τότε κάθε μία από τις $|A| - 1$ αλλοιώσεις έχει την ίδια πιθανότητα να συμβεί.

Ένας τέτοιος δίαυλος καλείται $|A|$-*αδικός συμμετρικός δίαυλος*.

Ας είναι $\Delta$ ένας συμμετρικός δυαδικός δίαυλος και ας υποθέσουμε ότι μία λέξη $x$ μήκους $n$ μεταδίδεται διά μέσου του $\Delta$. Τότε η πιθανότητα να υπάρξει λάθος σε $i$ συγκεκριμένες θέσεις της $x$ είναι $p^i(1-p)^{n-i}$ $(i = 0, \ldots, n)$. Άρα, καθώς $p < 1/2$, η πιθανότητα να μην υπεισέλθει λάθος σε $i$ συγκεκριμένες θέσεις της $x$ είναι μεγαλύτερη από την πιθανότητα να υπάρξει λάθος.

## 1.2 Απόσταση του *Hamming*

Ας είναι $A$ ένα αλφάβητο και $x = (x_1, \ldots, x_n)$, $y = (y_1, \ldots, y_n)$ δύο λέξεις μήκους $n$ με στοιχεία από το $A$.

**Ορισμός 1.1** Καλούμε *απόσταση του Hamming* των λέξεων $x$ και $y$ το πλήθος των θέσεων $i$ με $x_i \neq y_i$. Η απόσταση του Hamming των $x$ και $y$ συμβολίζεται με $\mathrm{d}(x, y)$.

Για παράδειγμα, αν $x = (1, 0, 0, 0, 1, 1)$ και $y = (0, 1, 1, 1, 0, 1)$, τότε $\mathrm{d}(x, y) = 5$.

**Πρόταση 1.1** *Για κάθε $x, y, z \in A^n$ ισχύουν τα εξής:*
*(α)* $\mathrm{d}(x, y) \geq 0$.
*(β)* $\mathrm{d}(x, y) = 0$ *αν και μόνον αν* $x = y$.
*(γ)* $\mathrm{d}(x, y) = \mathrm{d}(y, x)$.
*(δ)* $\mathrm{d}(x, y) \leq \mathrm{d}(x, z) + \mathrm{d}(y, z)$.

*Απόδειξη.* Οι τρείς πρώτες ιδιότητες είναι προφανείς. Θ΄ αποδείξουμε την τέταρτη. Ας είναι λοιπόν $x = (x_1, \ldots, x_n)$, $y = (y_1, \ldots, y_n)$ και $z = (z_1, \ldots, z_n)$. Θεωρούμε τα σύνολα

$$S = \{i/\ x_i \neq y_i,\ x_i = z_i\} \quad \text{και} \quad T = \{i/\ x_i \neq y_i,\ x_i \neq z_i\}.$$

Τότε $\mathrm{d}(x,y) = |S| + |T|$. Από την άλλη πλευρά έχουμε $|T| \leq \mathrm{d}(x,z)$. Επίσης, αν $i \in S$, τότε $y_i \neq z_i$, απ'οπου έπεται ότι $|S| \leq \mathrm{d}(y,z)$. Άρα $\mathrm{d}(x,y) \leq \mathrm{d}(x,z) + \mathrm{d}(y,z)$.

Από τις ιδιότητες (α)-(δ) έπεται ότι το σύνολο $A^n$ εφοδιασμένο με την συνάρτηση $\mathrm{d}(x,y)$ είναι ένας μετρικός τοπολογικός χώρος. Αν $x$ είναι λέξη ενός κώδικα η οποία μετά την διέλευση της από ένα δίαυλο μετασχηματίζεται στη $y$, τότε η ποσότητα $\mathrm{d}(x,y)$ δίνει το πλήθος των λαθών που έχουν υπεισέλθει στη $x$ και την έχουν μεταβάλλει σε $y$.

**Ορισμός 1.2** Κάθε υποσύνολο $C$ του $A^n$ καλείται *κώδικας μήκους* $n$ επί του $A$. Αν $|A| = q$, τότε ο κώδικας $C$ καλείται *$q$-αδικός*.

**Παράδειγμα 1.5** Το σύνολο $C$ που αποτελείται από τις λέξεις

$$e_0 = (0,0,0),\ e_1 = (0,1,1),\ e_2 = (1,0,1),\ e_3 = (1,1,0)$$

είναι ένας κώδικας μήκους 3 επί του αλφαβήτου $B$. Παρατηρούμε ότι η απόσταση του Hamming μεταξύ δύο λέξεων του $C$ ισούται με 2.

**Ορισμός 1.3** Καλούμε *ελάχιστη απόσταση* ενός κώδικα $C$ και την συμβολίζουμε με $\mathrm{d}(C)$, την μικρότερη απόσταση μεταξύ δύο διαφορετικών λέξεων του $C$. Δηλαδή,

$$\mathrm{d}(C) = \min\{\mathrm{d}(x,y)/\ x,y \in C,\ x \neq y\}.$$

Για παράδειγμα, η ελάχιστη απόσταση του κώδικα $C$ στο προηγούμενο παράδειγμα είναι 2.

Ένας κώδικας $C$ μήκους $n$ με $M$ λέξεις και ελάχιστη απόσταση $d$ θα αναφέρεται για συντομία ως ένας $(n,M,d)$-κώδικας. Αν $x \in \mathbb{R}$, τότε συμβολίζουμε με $\lfloor x \rfloor$ τον μεγαλύτερο ακέραιο $\leq x$.

**Πρόταση 1.2** *Ας είναι $C$ ένας κώδικας μήκους $n$ επί του $A$ με ελάχιστη απόσταση $d$. Τότε για κάθε $y \in A^n$ υπάρχει το πολύ μία λέξη $x \in C$ με $\mathrm{d}(x,y) \leq \lfloor (d-1)/2 \rfloor$.*

*Απόδειξη.* Ας είναι $e = \lfloor (d-1)/2 \rfloor$. Αν $x_1, x_2 \in C$ με $\mathrm{d}(x_1,y) \leq e$ και $\mathrm{d}(x_2,y) \leq e$, τότε έχουμε

$$\mathrm{d}(x_1,x_2) \leq \mathrm{d}(x_1,y) + \mathrm{d}(x_2,y) \leq 2e < d$$

που είναι άτοπο.

Συνήθως, για την επιλογή του κώδικα που θα χρησιμοποιηθεί για την κωδικοποίηση της πληροφορίας η οποία θα διέλθει από ένα συγκεκριμένο δίαυλο $\Delta$, γίνεται στατιστική ανάλυση του πλήθους των λαθών που παρουσιάζουν τα μηνύματα που διέρχονται από αυτόν. Στη περίπτωση όπου η πιθανότητα αυτός ο αριθμός να είναι $> e$ είναι πολύ μικρή, επιλέγεται ένας κώδικας $C$ με ελάχιστη απόσταση $d$ τέτοια, ώστε $\lfloor (d-1)/2 \rfloor = e$.

Η μέθοδος αποκωδικοποίησης των λαμβανομένων λέξεων διά μέσου του $\Delta$ γίνεται με την *αρχή της πλησιέστερης λέξης*. Σύμφωνα μ΄ αυτή μία λέξη $y$ αποκωδικοποιείται με τον εξής τρόπο. Αν $y \in C$, τότε η αποκωδικοποίηση της $y$ είναι η ίδια η $y$. Ας υποθέσουμε ότι $y \notin C$. Τότε υπολογίζουμε την ποσότητα

$$\delta = \min\{\mathrm{d}(y,z)/\ z \in C\}.$$

Αν υπάρχει μόνο μία λέξη $z \in C$ με $\mathrm{d}(y,z) = \delta$, τότε η αποκωδικοποίηση της $y$ είναι η $z$. Αν υπάρχουν περισσότερες της μίας λέξης του $C$ μ΄ αυτή την ιδιότητα, τότε είτε λαμβάνουμε ως αποκωδικοποίηση της $y$ κάποια από αυτές με τυχαίο τρόπο, είτε ζητάμε επαναμετάδοση της λέξης.

Ας υποθέσουμε ότι η $y$ έχει προέλθει από την λέξη $x \in C$ μετά την διέλευσή της διά μέσου του $\Delta$. Σύμφωνα με την Πρόταση 1.2, υπάρχει το πολύ ένα $z \in C$ τέτοιο, ώστε $\mathrm{d}(z,y) \leq e$. Έτσι, στη περίπτωση όπου $\mathrm{d}(x,y) \leq e$, έχουμε $x = z$. Άρα, αν στη λέξη $x$ έχουν εμφανιστεί το πολύ $e$ λάθη, τότε η παραπάνω μέθοδος αποκωδικοποίησης την διορθώνει. Καθώς η πιθανότητα εμφάνισης περισσότερων των $e$ λαθών σε μία λέξη που μεταδίδεται διά μέσου του $\Delta$ είναι πολύ μικρή, η πιθανότητα της επιτυχούς διόρθωσης μιας αλλοιωμένης λέξης μ΄ αυτό τον τρόπο είναι πολύ μεγάλη.

Στη συνέχεια, ας υποθέσουμε ότι η $y$ έχει προκύψει από την $x$ κατόπιν εμφάνισης $2e$ το πολύ λαθών, δηλαδή $\mathrm{d}(x,y) \leq 2e$. Οπότε, καθώς η απόσταση μεταξύ δύο λέξεων του $C$ είναι τουλάχιστον $d > 2e$, έπεται ότι η $y$ δεν είναι λέξη του $C$ και κατά συνέπεια ανιχνεύεται η εμφάνιση λαθών κατά την μετάδοση.

Αν το πλήθος των λαθών είναι $> e$ τότε είναι δυνατό να υπάρχει λέξη $z \in C$ με $z \neq x$ και $\mathrm{d}(x,y) = \mathrm{d}(z,y)$. Ένα τέτοιο παράδειγμα δίνουμε παρακάτω.

**Παράδειγμα 1.6** Ας είναι $C$ ο κώδικας του Παραδείγματος 1.5. Έχουμε $\mathrm{d}(C) = 2$ και $e = \lfloor (d-1)/2 \rfloor = 0$. Οπότε, ο $C$ δεν μπορεί να διορθώσει κανένα λάθος. Ας υποθέσουμε ότι η λέξη $(0,1,1)$ μεταδίδεται διά μέσου ενός διαύλου και λαμβάνεται η λέξη $(1,1,1)$ που δεν ανήκει στο $C$. Έτσι, το λάθος αν και έγινε αντιληπτό, δεν είναι δυνατό να διορθωθεί γιατί η απόσταση της $(1,1,1)$ από τρείς λέξεις του $C$ είναι ίδια.

**Ορισμός 1.4** Ας είναι $C$ ένας κώδικας με ελάχιστη απόσταση $d$. Ο αριθμός $\lfloor (d-1)/2 \rfloor$ καλείται *ικανότητα διόρθωσης* του $C$.

**Παράδειγμα 1.7** Ας είναι $q$ ακέραιος $> 0$ και $A = \{x_1, \ldots, x_q\}$. Ο *$q$-αδικός κωδικας επανάληψης* μήκους $n$ επί του $A$ είναι το υποσύνολο $E_n$ του $A^n$ που αποτελείται από τις λέξεις

$$(x_1, \ldots, x_1), \ldots, (x_q, \ldots, x_q).$$

Παρατηρούμε ότι η ελάχιστη απόσταση του $E_n$ είναι $n$. Οπότε, η ικανότητα διόρθωσης του $E_n$ είναι $\lfloor (n-1)/2 \rfloor$.

**Παράδειγμα 1.8** Σύμφωνα με το Παράδειγμα 1.2, οι λέξεις του κώδικα ISBN είναι ολές οι δεκάδες $(x_1, \ldots, x_{10})$, με $x_1, \ldots, x_9 \in \{0, \ldots, 9\}$ και $x_{10} \in \{0, \ldots, 10\}$, που ικανοποιούν την σχέση

$$x_{10} \equiv \sum_{i=1}^{9} i x_i \pmod{11}.$$

Επίσης, διαπιστώσαμε ότι αν μεταβληθεί ένα μόνο από τα γράμματα μίας λέξης του κώδικα, τότε η λέξη που προκύπτει δεν ανήκει στον κώδικα. Ας είναι $x = (x_1, \ldots, x_{10})$ μία λέξη του κώδικα ISBN. Αν $z_1 \in \{0, \ldots, 9\}$ με $x_1 \neq z_1$ και $z_{10} \in \{0, \ldots, 10\}$ με

$$z_{10} \equiv z_1 + \sum_{i=2}^{9} i x_i \pmod{11},$$

τότε η λέξη $z = (z_1, x_2, \ldots, x_9, z_{10})$ ανήκει στον κώδικα και $\mathrm{d}(x, z) = 2$. Άρα, η ελάχιστη απόσταση του κώδικα ISBN είναι 2 και επομένως η ικανότητα διόρθωσής του 0. Επίσης, όπως είδαμε, στην περίπτωση εμφάνισης ενός μόνο λάθους έχει την δυνατότητα να το ανιχνεύει.

**Παράδειγμα 1.9** Όπως είδαμε στο Παράδειγμα 1.3, οι λέξεις του κώδικα ASCII είναι τα στοιχεία του συνόλου $B^8$ των οποίων το πλήθος των 1 είναι άρτιο. Άρα, κάθε μη μηδενική λέξη θα περιέχει τουλάχιστον δύο 1. Αν σε μία τέτοια λέξη αντικαταστήσουμε δύο 1 με 0, τότε παίρνουμε πάλι μία λέξη του κώδικα. Από την άλλη πλευρά, δύο λέξεις του κώδικα δεν μπορούν να διαφέρουν μεταξύ τους κατά ένα γράμμα γιατί τότε μία από αυτές δεν θα έχει άρτιο πλήθος 1 που είναι άτοπο. Συνεπώς, η ελάχιστη απόσταση του κώδικα ASCII είναι 2. Οπότε, η ικανότητα διόρθωσής του είναι 0 και, όπως έχουμε ήδη δεί, στη περίπτωση εμφάνισης ενός μόνο λάθους έχει την δυνατότητα να το ανιχνεύει.

**Παράδειγμα 1.10** Όπως είδαμε στο Παράδειγμα 1.4, οι λέξεις του τριπλού κώδικα ελέγχου είναι τα στοιχεία $(a, b, c, x, y, z)$ του $B^6$ που είναι τέτοια, ώστε οι τριάδες $(a, b, x)$, $(a, c, y)$ και $(b, c, z)$ να έχουν άρτιο πλήθος 1. Επίσης, αν δύο γράμματα μίας λέξης του κώδικα μεταβληθούν, τότε η λέξη που προκύπτει δεν ανήκει πλέον στον κώδικα. Οι λέξεις $A = (1, 1, 0, 0, 1, 1)$ και $B = (0, 1, 0, 1, 0, 1)$ ανήκουν στον κώδικα και ισχύει $\mathrm{d}(A, B) = 3$. Άρα, η ελάχιστη απόσταση του κώδικα είναι 3. Επομένως, η ικανότητα διόρθωσής του είναι 1 και στην περίπτωση εμφάνισης δύο το πολύ λαθών έχει την δυνατότητα να τα ανιχνεύει.

## 1.3 Τέλειοι Κώδικες

Ας είναι $A$ ένα αλφάβητο και $n$ ένας θετικός ακέραιος.

**Ορισμός 1.5** Αν $r$ είναι θετικός ακέραιος και $x \in A^n$, τότε καλούμε *σφαιρική περιοχή* κέντρου $x$ και ακτίνας $r$ το σύνολο

$$B(x, r) = \{y \in A^n / \ \mathrm{d}(x, y) \leq r\}.$$

Ας είναι $C$ ένας κώδικας μήκους $n$ επί του $A$ με ικανότητα διόρθωσης $e$. Τότε για κάθε $x, y \in C$ με $x \neq y$ έχουμε $\mathrm{d}(x, y) > 2e$ και επομένως $B(x, e) \cap B(y, e) = \emptyset$.

**Ορισμός 1.6** Ο κώδικας $C$ καλείται *τέλειος*, αν ισχύει

$$\bigcup_{x \in C} B(x, e) = A^n.$$

Στην περίπτωση όπου ο κώδικας $C$ είναι τέλειος, οι σφαιρικές περιοχές με κέντρα τις λέξεις του $C$ και ακτίνα $e$ αποτελούν μία διαμέριση του $A^n$. Δηλαδή, ικανοποιούν τις εξής ιδιότητες:
(α) $B(x,e) \neq \emptyset$, για κάθε $x \in C$.
(β) $B(x,e) \cap B(y,e) = \emptyset$, για κάθε $x, y \in C$ και $x \neq y$.
(γ) $\cup_{x \in C} B(x,e) = A^n$.

Συνεπώς, για κάθε $y \in A^n$ υπάρχει ακριβώς ένα $x \in C$ τέτοιο, ώστε $y \in B(x,e)$. Οπότε, αν διά μέσου ενός διαύλου επικοινωνίας λαμβάνεται μία λέξη $y \in A^n \setminus C$, τότε προσδιορίζεται η μοναδική λέξη $x \in C$ με $y \in B(x,e)$. Η λέξη $x$ λαμβάνεται ως αποκωδικοποίηση της $y$. Έτσι, κάθε λέξη αποκωδικοποιείται με μοναδικό τρόπο. Αυτό όμως δεν συμβαίνει στην περίπτωση όπου ο κώδικας δεν είναι τέλειος, όπως δείχνει το παρακάτω παράδειγμα.

**Παράδειγμα 1.11** Θεωρούμε τον κώδικα $C$ μήκους 5 επί του $B$ που αποτελείται από τις λέξεις

$$x = (0,1,1,1,0),\ y = (1,0,1,0,1),\ z = (1,1,0,1,1).$$

Η ελάχιστη απόσταση του $C$ είναι 3 και επομένως η ικανότητα διόρθωσής του ισούται με 1. Οι σφαιρικές περιοχές με κέντρα τις λέξεις του $C$ και ακτίνα 1 είναι:

$$\begin{aligned} B(x,1) = \{&(0,1,1,1,0),(1,1,1,1,0),(0,0,1,1,0),\\ &(0,1,0,1,0),(0,1,1,0,0),(0,1,1,1,1)\}, \end{aligned}$$

$$\begin{aligned} B(y,1) = \{&(1,0,1,0,1),(0,0,1,0,1),(1,1,1,0,1),\\ &(1,0,0,0,1),(1,0,1,1,1),(1,0,1,0,0)\}, \end{aligned}$$

$$\begin{aligned} B(z,1) = \{&(1,1,0,1,1),(0,1,0,1,1),(1,0,0,1,1),\\ &(1,1,1,1,1),(1,1,0,0,1),(1,1,0,1,0)\}. \end{aligned}$$

Παρατηρούμε ότι η ένωση των τριών σφαιρικών περιοχών δεν δίνει το $B^5$. Πράγματι, η λέξη $u = (1,0,1,1,0)$ δεν ανήκει σε καμμία από αυτές. Άρα, ο κώδικας $C$ δεν είναι τέλειος. Επίσης, έχουμε $\mathrm{d}(x,u) = 2 = \mathrm{d}(y,u)$ και $\mathrm{d}(z,u) = 3$. Οπότε, αν για την αποκωδικοποίηση του $u$ επιλέξουμε την πιο κοντινή λέξη του $C$, τότε βλέπουμε ότι υπάρχουν δύο τέτοιες μ΄ αυτή την ιδιότητα και επομένως η αποκωδικοποίηση του $u$ δεν γίνεται με μοναδικό τρόπο.

Στη συνέχεια θα υπολογίσουμε το πλήθος των λέξεων που περιέχεται μέσα σε μία σφαιρική περιοχή. Γι΄ αυτό τον σκοπό θα χρειαστούμε το παρακάτω λήμμα.

**Λήμμα 1.1** *Για κάθε $x \in A^n$ και κάθε θετικό ακέραιο $r \leq n$ ισχύει*

$$|B(x,r)| = \sum_{i=0}^{r} (|A|-1)^i \begin{pmatrix} n \\ i \end{pmatrix}.$$

*Απόδειξη.* Θεωρούμε τα σύνολα

$$S(x,i) = \{y \in A^n / \ \mathrm{d}(x,y) = i\} \quad (i = 1, \ldots, r).$$

Θα υπολογίσουμε το πλήθος των λέξεων του $S(x,i)$. Μία λέξη $y \in S(x,i)$ αν και μόνον αν το πλήθος των γραμμάτων του $y$ που διαφέρουν από τα αντίστοιχα γράμματα του $x$ είναι $i$. Το πλήθος των επιλογών γι΄ αυτά τα $i$ γράμματα είναι

$$\begin{pmatrix} n \\ i \end{pmatrix}.$$

Επίσης, κάθε τέτοιο γράμμα μπορεί να πάρει $|A|-1$ διαφορετικές τιμές. Άρα

$$|S(x,i)| = (|A|-1)^i \begin{pmatrix} n \\ i \end{pmatrix}$$

και επομένως

$$|B(x,r)| = \sum_{i=0}^{r} |S(x,i)| = \sum_{i=0}^{r} (|A|-1)^i \begin{pmatrix} n \\ i \end{pmatrix}.$$

**Πρόταση 1.3** *(Φράγμα του Hamming) Αν $C$ είναι ένας κώδικας μήκους $n$ επί του $A$ με ικανότητα διόρθωσης $e$. Τότε*

$$|C| \sum_{i=0}^{e} (|A|-1)^i \begin{pmatrix} n \\ i \end{pmatrix} \leq |A|^n.$$

*Η ισότητα ισχύει αν και μόνον αν ο $C$ είναι τέλειος.*

*Απόδειξη.* Για κάθε $x, y \in C$ ισχύει $B(x,e) \cap B(y,e) = \emptyset$. Άρα

$$\sum_{x \in C} |B(x,e)| \leq |A|^n$$

και η ισότητα ισχύει αν και μόνον αν ο $C$ είναι τέλειος. Από το Λήμμα 1.1 έχουμε ότι για κάθε $x \in C$ ισχύει

$$|B(x,e)| = \sum_{i=0}^{e} (|A|-1)^i \left( \begin{array}{c} n \\ i \end{array} \right).$$

Επομένως

$$|C| \sum_{i=0}^{e} (|A|-1)^i \left( \begin{array}{c} n \\ i \end{array} \right) \leq |A|^n$$

και η ισότητα ισχύει αν και μόνον αν ο $C$ είναι τέλειος.

**Παράδειγμα 1.12** Ο δυαδικός κώδικας επανάληψης μήκους $n$, όπου $n$ περιττός θετικός ακέραιος, είναι τέλειος κώδικας. Πράγματι, η ικανότητα διόρθωσής του είναι $(n-1)/2$ και έχουμε

$$2 \sum_{i=0}^{(n-1)/2} \left( \begin{array}{c} n \\ i \end{array} \right) = \sum_{i=0}^{(n-1)/2} \left( \begin{array}{c} n \\ i \end{array} \right) + \sum_{i=(n+1)/2}^{n} \left( \begin{array}{c} n \\ i \end{array} \right) = 2^n.$$

Επομένως, σύμφωνα με την Πρόταση 1.3, αυτός ο κώδικας είναι τέλειος.

## 1.4 Ισοδυναμία Κωδίκων

Ας είναι $A$ αλφάβητο και $n$ θετικός ακέραιος. Για κάθε μετάθεση $\sigma$ του συνόλου $\{1,\ldots,n\}$ ορίζουμε την απεικόνιση

$$f_\sigma : A^n \longrightarrow A^n,\ (x_1,\ldots,x_n) \longmapsto (x_{\sigma(1)},\ldots,x_{\sigma(n)})$$

και για κάθε αμφίεση $\tau : A \to A$ την απεικόνιση

$$f_i^\tau : A^n \longrightarrow A^n,\ (x_1,\ldots,x_i,\ldots,x_n) \longmapsto (x_1,\ldots,\tau(x_i),\ldots,x_n).$$

Παρατηρούμε ότι οι δύο απεικονίσεις $f_\sigma$ και $f_i^\tau$ είναι αμφιέσεις.

**Ορισμός 1.7** Δύο κώδικες $C_1$ και $C_2$ μήκους $n$ επί του $A$ καλούνται *ισοδύναμοι*, αν υπάρχει απεικόνιση $h : A^n \to A^n$ η οποία είναι σύνθεση απεικονίσεων της μορφής $f_\sigma$ και $f_i^\tau$, ώστε να ισχύει $h(C_1) = C_2$.

Εύκολα διαπιστώνουμε ότι η ισοδυναμία κωδίκων είναι μία σχέση ισοδυναμίας επί του συνόλου των κωδίκων του $A^n$. Επίσης, παρατηρούμε ότι για κάθε $x, y \in A^n$ ισχύει

$$\mathrm{d}(x,y) = \mathrm{d}(f_\sigma(x), f_\sigma(y)) = \mathrm{d}(f_i^\tau(x), f_i^\tau(y)).$$

Επομένως, δύο ισοδύναμοι κώδικες έχουν την ίδια ελάχιστη απόσταση.

**Παράδειγμα 1.13** Ας θεωρήσουμε τους κώδικες

$$C_1 = \{(0,0,1,0,0), (0,0,0,1,1), (1,1,1,1,1), (1,1,0,0,0)\}$$

και

$$C_2 = \{(0,0,0,0,0), (0,1,1,0,1), (1,0,1,1,0), (1,1,0,1,1)\}.$$

Θα δείξουμε ότι οι $C_1$ και $C_2$ είναι ισοδύναμοι. Ας είναι $\tau : B \to B$ με $\tau(0) = 1$ και $\tau(1) = 0$. Τότε

$$f_3^\tau(0,0,1,0,0) = (0,0,0,0,0), \quad f_3^\tau(0,0,0,1,1) = (0,0,1,1,1),$$

$$f_3^\tau(1,1,1,1,1) = (1,1,0,1,1), \quad f_3^\tau(1,1,0,0,0) = (1,1,1,0,0).$$

Αν $\sigma$ είναι η μετάθεση του $\{1,2,3,4,5\}$ με $\sigma(2) = 4$, $\sigma(4) = 2$, $\sigma(1) = 1$, $\sigma(3) = 3$, $\sigma(5) = 5$, τότε εφαρμόζουμε την αμφίεση $f_\sigma$ στον κώδικα $f_3^\tau(C_1)$ και παίρνουμε $f_\sigma(f_3^\tau(C_1)) = C_2$. Άρα, οι κώδικες $C_1$ και $C_2$ είναι ισοδύναμοι.

**Πρόταση 1.4** *Ας είναι $C$ κώδικας μήκους $n$ επί του αλφαβήτου $A = \{0,1,\ldots,q-1\}$. Τότε ο $C$ είναι ισοδύναμος μ΄ έναν κώδικα που περιέχει την λέξη $(0,\ldots,0)$.*

*Απόδειξη.* Ας είναι $(x_1,\ldots,x_n)$ μία τυχούσα λέξη του κώδικα και $\tau_i : A \to A$ η απεικόνιση με $\tau_i(0) = x_i$, $\tau_i(x_i) = 0$ και $\tau_i(y) = y$ για κάθε $y \in A \setminus \{0, x_i\}$. Οπότε, έχουμε

$$(f_1^{\tau_1} \circ \cdots \circ f_n^{\tau_n})(x_1,\ldots,x_n) = (0,\ldots,0).$$

Έτσι, ο κώδικας $(f_1^{\tau_1} \circ \cdots \circ f_n^{\tau_n})(C)$ περιέχει την λέξη $(0,\ldots,0)$ και είναι ισοδύναμος με τον $C$.

**Παράδειγμα 1.14** Ας είναι $C$ ένας κώδικας μήκους 5 επί του $B$ με $\mathrm{d}(C) = 3$ και $|C| \geq 4$. Σύμφωνα με την Πρόταση 1.4, υπάρχει κώδικας $C_1$ ισοδύναμος με τον $C$ και $(0,0,0,0,0) \in C_1$. Επίσης, ισχύει $\mathrm{d}(C_1) = \mathrm{d}(C) = 3$. Αν ο $C_1$ έχει δύο λέξεις $x$ και $y$ με τέσσερα ή πέντε 1, τότε $\mathrm{d}(x,y) \leq 2$ που είναι άτοπο. Άρα, ο $C_1$ έχει το πολύ μία λέξη με τέσσερα ή πέντε 1. Καθώς $(0,0,0,0,0) \in C_1$, ο $C_1$ δεν έχει λέξη που να περιέχει ακριβώς ένα ή δύο 1. Επίσης, υπάρχουν τουλάχιστον δύο

λέξεις του $C_1$ οι οποίες έχουν ακριβώς τρία 1 γιατί $|C_1| \geq 4$. Οπότε, χωρίς βλάβη της γενικότητας, ο $C_1$ περιέχει τις λέξεις

$$(0,0,0,0,0), \quad (1,1,1,0,0), \quad (0,0,1,1,1).$$

Δοκιμάζοντας όλες τις δυνατές περιπτώσεις, συμπεραίνουμε ότι ο $C_1$ περιέχει επιπλέον μόνο την λέξη $(1,1,0,1,1)$. Ο $C_1$ είναι ένας $(5,4,3)$-κώδικας και κατά συνέπεια, υπάρχει μόνο μία κλάση ισοδυναμίας δυαδικών $(5,4,3)$-κωδίκων. Επιπλέον, δεν υπάρχει δυαδικός $(5,M,3)$-κώδικας με $M > 4$.

## 1.5 Ασκήσεις

1. Ας είναι $C$ ένας κώδικας μήκους 3 επί ενός αλφαβήτου $A$ με $|A| = 3$. Αν $\mathrm{d}(C) = 2$, τότε να δειχθεί ότι $|C| \leq 9$. Επίσης, να κατασκευαστεί ένας τέτοιος κώδικας με $|C| = 9$.

2. Να δειχθεί ότι υπάρχει μόνο μία κλάση ισοδυναμίας δυαδικών $(8,4,5)$-κωδίκων.

3. Να δειχθεί ότι αν υπάρχει ένας δυαδικός κώδικας $C$ με μήκος $n$ και ελάχιστη απόσταση $d$, όπου $d$ άρτιος, τότε υπάρχει ένας δυαδικός κώδικας $C_1$ με μήκος $n$, ελάχιστη απόσταση $d$ και $|C| = |C_1|$ τέτοιος, ώστε οι λέξεις του να έχουν άρτιο πλήθος 1.

4. Να δειχθεί ότι κάθε $q$-αδικός κώδικας μήκους $n$ με $q$ στοιχεία και ελάχιστη απόσταση $n$ είναι ισοδύναμος με τον $q$-αδικό κώδικα επανάληψης μήκους $n$.

5. Ας είναι $C$ ένας δυαδικός κώδικας μήκους 8. Αν ο $C$ έχει ικανότητα διόρθωσης $e = 1$, τότε να δειχθεί ότι $|C| \leq 28$.

6. Ας είναι ο κώδικας

$$C = \{(0,1,1,0,1), (0,0,0,1,1), (1,0,1,1,0), (1,1,0,0,0)\}.$$

Ν′ αποκωδικοποιηθούν οι λέξεις

$$(0,0,0,0,0), (0,1,1,1,1), (1,0,1,1,0), (1,0,0,1,1), (1,1,0,1,1),$$

σύμφωνα με την μέθοδο της Ενότητας 1.2.

7. Θεωρούμε τον τριαδικό κώδικα

$$C = \{(0,0,1,2,2), (1,2,2,0,1), (2,0,1,1,0), (2,2,0,0,0)\}$$

Ν′ αποκωδικοποιηθούν οι λέξεις

$$(0,1,1,2,2), (1,0,0,2,1), (2,2,0,2,2), (2,0,1,2,0),$$

σύμφωνα με την μέθοδο της Ενότητας 1.2.

8. Ας είναι

$$C = \{(0,0,0,0), (1,0,0,1), (0,1,1,0), (1,1,1,1)\}.$$

Να προσδιοριστούν οι λέξεις που μπορεί να διορθώσει ο κώδικας $C$.

9. Δείξτε ότι οι κώδικες

$$C = \{(1,2,0), (1,0,2), (2,1,0), (1,1,0), (2,1,2)\}$$

και

$$D = \{(0,0,0), (0,2,2), (2,1,0), (0,1,0), (2,1,2)\}$$

είναι ισοδύναμοι.

10. Οι αριθμοί ISBN

$$0-13-1\bullet 9139-9 \quad \text{και} \quad 0-02-32\bullet\bullet 80-0$$

έχουν ληφθεί, όπου οι μαύρες κουκίδες συμβολίζουν τα ψηφία τους που καταστράφηκαν κατά την μετάδοση. Ποιά είναι τα ψηφία που λείπουν;