Δημήτριος Α. Βάρσος

Στοιχεία Αλγεβρικής Θεωρίας Κωδίκων

ΑΘΗΝΑ 2005

Στον Αθανάσιο και στη Δήμητρα

Περιεχόμενα

Πρόλογος **1**

1 Βασικές Έννοιες **5**
1.1 Τί είναι κώδικας 5
1.2 Ορισμοί και στοιχειώδεις ιδιότητες 6
1.2.1 Κωδικοποίηση - Αποκωδικοποιήση 8
1.2.2 Το πρόβλημα της αποκωδικοποίησης 14
1.2.3 Ασκήσεις 16
1.3 Κανόνες Αποκωδικοποίησης 17
1.3.1 Η αρχή της αποκωδικοποίησης μέγιστης πιθανότητας . . . 19
1.3.2 Η Αρχή της αποκωδικοποίησης ως προς την πλησιέστερη λέξη 22
1.3.3 Ταυτόχρονη ανίχνευση και διόρθωση λαθών 31
1.3.4 Ασκήσεις 32
1.4 Κώδικες που προέρχονται από άλλους κώδικες 34
1.4.1 Μερικές περιπτώσεις "μετασκευής " κωδίκων 34
1.4.2 Μεγιστικοί κώδικες 42
1.4.3 Ασκήσεις 43
1.5 Τέλειοι κώδικες 45
1.5.1 Σφαίρες ομαδοποίησης και τέλειοι κώδικες 45
1.5.2 Φράγματα κωδίκων 51
1.5.3 Ασκήσεις 55

2 Γραμμικοί Κώδικες **57**
2.1 Η έννοια του Γραμμικού κώδικα. 57
2.1.1 Γεννήτορες πίνακες ενός Γραμμικού κώδικα. 59
2.1.2 Ασκήσεις 64
2.2 Δυϊκοί κώδικες 65

2.2.1 Κώδικες που προέρχονται από άλλους κώδικες (Η περίπτωση των γραμμικών κωδίκων) . . . 73
2.2.2 Αυτοδυϊκοί κώδικες . . . 75
2.2.3 Υπολογισμός της ελάχιστης απόστασης σε ένα γραμμικό κώδικα . . . 77
2.2.4 Άσκήσεις . . . 80
2.3 Κωδικοποίηση και αποκωδικοποίηση με γραμμικούς κώδικες . . . 81
2.3.1 Διόρθωση λαθών με έναν γραμμικό κώδικα . . . 81
2.3.2 Η πιθανότητα σωστής αποκωδικοποίησης με έναν γραμμικό κώδικα . . . 86
2.3.3 Ανίχνευση λαθών με έναν γραμμικό κώδικα . . . 87
2.3.4 Το σύνδρομο σε έναν γραμμικό κώδικα . . . 89
2.3.5 Ασκήσεις . . . 93
2.4 Διασπορά βαρών σε έναν κώδικα . . . 94
2.4.1 Ασκήσεις . . . 96
2.5 Κώδικες με μέγιστη απόσταση (MDS Κώδικες) . . . 97
2.5.1 Ασκήσεις . . . 103
2.6 Μερικές κατηγορίες γραμμικών κωδίκων . . . 103
2.6.1 Πολυωνυμικοί κώδικες . . . 104
2.6.2 Κυκλικοί κώδικες . . . 108
2.6.3 Ασκήσεις . . . 123

3 "Καλοί" Κώδικες **125**
3.1 Κώδικες Hamming . . . 125
3.1.1 Αποκωδικοποίηση με κώδικες Hamming . . . 128
3.1.2 Ο δυϊκός ενός κώδικα Hamming . . . 129
3.1.3 Οι κώδικες Hamming ως κυκλικοί κώδικες . . . 131
3.1.4 Ασκήσεις . . . 134
3.2 Κώδικες Golay . . . 135
3.2.1 Δυαδικοί κώδικες Golay . . . 135
3.2.2 Τριαδικοί κώδικες Golay . . . 139
3.2.3 Οι κώδικες Golay ως κυκλικοί κώδικες . . . 140
3.2.4 Ασκήσεις . . . 144
3.3 Η μοναδικότητα των κωδίκων Hamming και Goley ως τέλειοι κώδικες . . . 145
3.4 Κώδικες Reed-Muller . . . 149
3.4.1 Σύγκριση των κωδίκων Hamming και Reed-Muller . . . 151
3.4.2 Κώδικες Reed-Muller ανώτερης τάξης . . . 153
3.4.3 Ασκήσεις . . . 154

Α΄ Στοιχεία από την Άλγεβρα **155**
Α΄.1 Δακτύλιοι 155
Α΄.1.1 Ορισμοί και ιδιότητες 155
Α΄.1.2 Ομομορφισμοί-Ιδεώδη 161
Α΄.1.3 Επεκτάσεις σωμάτων 165
Α΄.2 Ο δακτύλιος των πολυωνύμων 166
Α΄.2.1 Διαιρετότητα πολυωνύμων 167
Α΄.2.2 Μέγιστος Κοινός Διαιρέτης Πολυωνύμων 170
Α΄.2.3 Ελάχιστο κοινό πολλαπλάσιο πολυωνύμων 176
Α΄.2.4 Ρίζες πολυωνύμων 179
Α΄.3 Πεπερασμένα Σώματα 183
Α΄.3.1 Τα πεπερασμένα σώματα ως σώματα ριζών πολυωνύμων . 183
Α΄.3.2 Τα υποσώματα ενός πεπερασμένου σώματος 184
Α΄.3.3 Ανάγωγα πολυώνυμα με συντελεστές από πεπερασμένα σώματα 187
Α΄.3.4 Οι ρίζες της μονάδας επί πεπερασμένων σωμάτων 192

Βιβλιογραφία **196**

Ευρετήριο **199**

Πρόλογος

Υπάρχουν πολλοί λόγοι που υπαγορεύουν την κωδικοποίηση δεδομένων, τα οποία πρόκειται να μεταδοθούν ή να αποθηκευθούν. Γενικά θα μπορούσαμε να τους κατατάξουμε σε τρείς μεγάλες κατηγορίες.

Ο πρώτος λόγος έχει σχέση με την *αποτελεσματικότητα στη διαχείρηση της πληροφορίας*. Όλοι γνωρίζουμε τη σημασία που έχει ο τρόπος, με τον οποίο *συμπιέζουμε* κάποια δεδομένα για να επιτύχουμε " οικονομία " χρόνου κατά τη μετάδοση, χώρου κατά την αποθήκευση, αλλά και "ευχέρεια " κατά την ανάκτηση και επεξεργασία. Ο δεύτερος λόγος έχει σχέση με την *προστασία* της πληροφορίας κατά τη μετάδοση μέσω ενός *θορυβώδους* διαύλου επικοινωνίας.

Τέλος ο τρίτος λόγος έχει σχέση με την *προστασία* της πληροφορίας από την πρόσβαση σ' αυτήν μη εξουσιοδοτημένων ατόμων.

Φυσικά ανά πάσα στιγμή ενδέχεται να συνυπάρχουν και οι τρείς λόγοι και ο διαχωρισμός γίνεται μόνο για τεχνικούς λόγους. Επομένως έχουμε τρείς κλάδους της επιστήμης που ασχολείται με την κωδικοποίηση. Την "Θεωρία της Πληροφορίας", την " Θεωρία κωδίκων" και την "Κρυπτογραφία".

Αν και η Κρυτογραφία έχει τις απαρχές της στην αρχαιότητα, θα μπορούσε να ισχυρισθεί κάποιος ότι από καταβολής κόσμου ο άνθρωπος είχε μυστικά τα οποία ήθελε να μοιράζεται με άτομα της δικής του επιλογής, η Θεωρία της Πληροφορίας και η Θεωρία Κωδίκων είναι νεώτατες και η γέννησή τους σηματοδοτείται από το περίφημο άρθρο του Claude Shannon "*Mathematical Theory of Communications*" το 1948. Έκτοτε υπήρξε μια *έκρηξη* ερευνητικών αποτελεσμάτων και *καταιγισμός* δημοσιεύσεων με αποτέλεσμα, πέραν των καθημερινών εφαρμογών, η Θεωρία της Πληροφορίας και η Θεωρία Κωδίκων να αναχθούν σε επιστήμη με υψηλό Μαθηματικό υπόβαθρο .

Η ξενόγλωσση βιβλιογραφία είναι εκτενής και το επίπεδο των συγγραμμάτων ποικίλλει από απλά και εκλαϊκευμένα μέχρι ακρώς θεωρητικά και ερευνητικού ενδιαφέροντος.

Η Ελληνόγλωσση βιβλιογραφία, αν όχι ανυπαρκτή, είναι πενιχρή.

Το "ανά χείρας" βιβλίο απευθύνεται κυρίως σε φοιτητές Θετικών Επιστημών και σκοπός του είναι να τους εισάγει στη Θεωρία Κωδίκων και ειδικότερα στην Αλγεβρική Θεωρία Κωδίκων. Παράλληλα όμως σκοπεύει να δείξει, ακόμα και στον ανυποψίαστο αναγνώστη, την αναγκαιότητα, τη δύναμη και την ωραιότητα των Μαθηματικών.

Το επίπεδο έχει επιλεγεί ούτως ώστε να είναι προσιτό ακόμη και σε άτομα χωρίς προηγούμενη (υψηλή) Μαθηματική παιδεία, τα οποία όμως είναι διατεθημένα να μελετήσουν τα "απαιτούμενα" Μαθηματικά. Έχει γίνει προσπάθεια η παρουσίαση να είναι απλή, αλλά όχι απλοϊκή και σε πολλά σημεία δίνονται ερεθίσματα για περαιτέρω μελέτη.

Το βιβλίο χωρίζεται σε τρία Κεφάλαια και ένα Παράρτημα. Πρόσπαθήσαμε ούτως ώστε οι επιμέρους παράγραφοι να είναι όσον το δυνατόν ανεξάρτητοι έτσι ώστε να εξασφαλίζεται μια ευελιξία ως προς τη σειρά κατά τη διάρκεια της μελέτης.

Στο πρώτο κεφάλαιο εκτός από τις βασικές έννοιες και ορισμούς γίνεται μια παρουσίαση των βασικών κατασκευών κωδίκων, της έννοιας του τέλειου κώδικα και μελετώνται ορισμένα φράγματα του μεγέθους ενός κώδικα σε συνάρτηση με τις υπόλοιπες παραμέτρους (μήκος και ελάχιστη απόσταση).

Το δεύτερο κεφάλαιο είναι αφιερωμένο στους Γραμμικούς Κώδικες. Εδώ γίνεται προσπάθεια να καταδειχθεί η σημασία της αλγεβρικής δομής των κωδίκων ως διανυσματικοί χώροι επί πεπερασμένων σωμάτων. Η γνωστή γεωμετρική έννοια της καθετότητας αποτελεί βασικό εργαλείο στον ορισμό και στη μελέτη του δυϊκού κώδικα ένος γραμμικού κώδικα. Όπως και στο σχεδιασμό μεθόδων για την διόρθωση λαθών μέσω ενός γραμμικού κώδικα.

Χρησιμοποιώντας απλές ιδιότητες του δακτυλίου πολωνύμων με συντελεστές από ένα πεπερασμένο σώμα εισάγονται οι πολυωνυμικοί και κυκλικοί κώδικες, η σημαντικώτερη ίσως κατηγορία κωδίκων. Η μελέτη των κωδίκων αυτών απαιτεί τη γνώση της έννοιας του ιδεώδους και του δακτυλίου πηλίκων. Εδώ ο αναγνώστης θα πρέπει να γνωρίζει (ή να φροντίσει τώρα να μελετήσει) και να χειρίζεται αυτές τις αλγεβρικές έννοιες με σχετική ευχέρεια.

Στο τρίτο κεφάλαιο παρουσιάζονται τρείς πολύ γνωστές κατηγορίες κωδίκων. Οι κώδικες αυτοί εκτός του ότι παρουσιάζουν πρακτικό και θεωρητικό ενδιαφέρον, αποτελούν μια ενδιαφέρουσα εφαρμογή όσων προηγήθηκαν στα προηγούμενα κεφάλαια.

Τέλος στο Παράρτημα παρατίθενται συνοπτικά οι αλγεβρικές έννοιες που απαιτούνται στα προηγούμενα Κεφάλαια. Το μέρος αυτό του βιβλίου **δεν** πρέπει να θεωρηθεί ως μια εισαγωγή στην Άλγεβρα. Παρατίθεται για να συμβάλλει στην αυτοτέλεια του βιβλίου και για διευκόλυνση του αναγνώστη, ο οποίος θα ανατρέχει σ' αυτό για να επαναφέρει στη μνήμη του έννοιες, τις οποίες (οφείλει

να) έχει διδαχθεί σε ένα μάθημα "Βασικής Άλγεβρας " προπτυχιακού επιπέδου.

Σε κάθε παράγραφο παρατίθενται πολλά παραδείγματα, όπως και αρκετές ασκήσεις. Επειδή πιστεύουμε στην ενεργή συμμετοχή του αναγνώστη κατά τη διάρκεια της μελέτης του, το κείμενο είναι διανθισμένο με εκφράσεις του τύπου *...εύκολα βλέπουμε ότι ..., ...δεν είναι δύσκολο να αποδείξουμε ότι.... .... η απόδειξη αποτελεί μια ωραία άσκηση ...,* όπως επίσης και πολλά *γιατί;*. Κατά τη γνώμη μας τα σημεία αυτά αποτελούν τις πλέον σημαντικές, για την κατανόηση, ασκήσεις και για το λόγο αυτό επιμένουμε ο αναγνώστης να προσπαθεί να διελευκάνει αυτού του είδους τα ερωτηματικά και το κυριώτερο, όπως (πρέπει να) συμβαίνει με τη μελέτη στα Μαθηματικά, να χρησιμοποιεί "μολύβι και χαρτί" κατά τη διάρκεια της μελέτης του.

Όπως προείπαμε, όχι μόνο δεν εξαντλούμε τον τεράστιο κλάδο της Αλγεβρικής Θεωρίας Κωδίκων, αλλά υπάρχουν ακόμα και πολύ σημαντικές περιοχές, οι οποίες ούτε καν αναφέρονται. Επιπλέον, επειδή πιστεύουμε ότι κατά την διάρκεια της μελέτης ενός αντικειμένου ο περιορισμός σε ένα μόνο σύγγραμμα (όσο καλό και αν είναι αυτό) *παγιδεύει* τον αναγνώστη. Η παρατειθέμενη ενδεικτική βιβλιογραφία θα βοηθήσει προς αποφυγή τέτοιων καταστάσεων και θα οδηγήσει τον ενδιαφερόμενο αναγνώστη σε περεταίρω μελέτη.

Τέλος, επειδή το καλύτερο βιβλίο είναι ....αυτό που δεν γράφτηκε .... . Το βιβλίο αυτό σίγουρα περιέχει λάθη και επιδέχεται βελτιώσεις. Θα θέλαμε να πιστεύουμε ότι: Τα *τυπογραφικά* λάθη είναι λίγα, τα γραματοικά και ωρθογραφεικά είναι λιγότερα, τα συντακτικά ελάχιστα και εκφραστικά . Κάθε υπόδειξη, διόρθωση που προέρχεται από καλοπροαίρετη (έστω αυστηρή) κριτική είναι ευπρόσδεκτη και οι ευχαριστίες προκαταβάλλονται... .

Μάρτιος 2005

Κεφάλαιο 1

Βασικές Έννοιες

Στο Κεφάλαιο αυτό εισάγουμε την έννοια του κώδικα και αναφέρουμε ορισμένες βασικές ιδιότητες, οι οποίες είναι απαραίτητες για τα επόμενα.

1.1 Τί είναι κώδικας

Όλοι έχουμε ακούσει για κώδικες, για κωδικοποιημένα μηνύματα, για κρυπτογράφηση και αποκρυπτογράφιση μηνυμάτων και άλλα σχετικά. Λίγοι όμως έχουν συνειδητοποιήσει ότι δεν υπάρχει άνθρωπος που να μην χρησιμοποιεί ανά πάσα στιγμή κώδικες.

Η γλώσσα που χρησιμοποιούμε για να επικοινωνούμε δεν είναι τίποτε άλλο παρά ένας κώδικας. Πράγματι κάθε τι που θέλουμε να εκφράσουμε προφορικώς ή γραπτώς το *κωδικοποιούμε* σε μία ακολουθία *λέξεων* χρησιμοποιώντας *γράμματα* από ένα *αλφάβητο*. Το σύνολο αυτών των λέξεων αποτελεί ένα *μήνυμα* το οποίο μεταδίδουμε προφορικώς, γραπτώς ή με κάποιο άλλο τρόπο.

Σε μια γλώσσα που έχει ένα αλφάβητο μπορούμε να σχηματίσουμε πάρα πολλές "λέξεις " (θεωρητικά άπειρες). Από αυτές όμως λίγες έχουν *νόημα*, δηλαδή αποτελούν στοιχεία του γλωσσικού κώδικα επικοινωνίας. Για το σχηματισμό των λέξεων που έχουν νόημα και γενικώτερα για τη συγκρότηση του γλωσσικού οικοδομήματος χρησιμοποιούνται κανόνες, όπως ορθογραφικοί, γραμματικοί, συντακτικοί κ.λ.π.

Κατά τη μετάδοση ένος μηνύματος με κάποιο τρόπο ενδέχεται (μερικώς) να αλλοιωθεί. Για παράδειγμα, αν η μετάδοση γίνεται προφορικά, ο ομιλητής (ο αποστολέας του μυνήματος) δεν έχει καλή άρθρωση, ο παραλήπτης δεν έχει καλή ακοή ή, το πιθανότερο, υπάρχουν θόρυβοι οι οποίοι παρεμβάλονται και παρεμποδίζουν τη σωστή λήψη του μυνήματος.

Αυτός που ακούει (ο παραλήπτης του μυνήματος) είναι αναγκασμένος να

συνάγει τί μήνυμα εστάλει από το μήνυμα που έλαβε (να *αποκωδικοποιήσει* το μήνυμα). Για βοήθεια έχει τον κώδικα γλωσσικής επικοινωνίας. Πολλές φορές είναι αναγκασμένος να εικάσει για το μήνυμα στηριζόμενος "στα συμφραζόμενα" ή ακόμα, αναλαμβάνοντας τον κίνδυνο για λανθασμένη απόδοση, να αποδόσει μέρος του μηνύματος τυχαία.

Ένα από τα χαρακτηριστικά ενός κώδικα γλωσσικής επικοινωνίας είναι ο πλούτος του λεξιλογίου του, που μας επιτρέπει να μπορούμε να μεταδόσουμε πολλά και σύνθετα νοήματα. Δηλαδή έχουμε τη δυνατότητα να μεταδόδουμε μεγάλο μέγεθος *πληροφορίας*. Άμεσα με το μέγεθος της πληροφορίας σχετίζεται και η ποιότητα της μεταδιδόμενης πληροφορίας καθώς επίσης και η οικονομία κατά τη μετάδοση. Οι δυνατότητες αυτές βεβαία καθορίζονται από τη *δομή* του γλωσσικού κώδικα. Οι απαιτήσεις αυτές, από την πλευρά τους, καθορίζουν ως ένα βαθμό το πώς θα αναπτυχθεί ένας γλωσσικός κώδικας για να είναι *αποτελεσματικός*. Δεν πρέπει όμως να αγνοείται το τρόπος επικοινωνίας, δηλαδή το μέσον που έχουμε στη διάθεσή μας για τη μετάδοση ενός μηνύματος. Το μέσο επικοινωνίας ορισμένες φορές επιβάλλει τον τρόπο με τον οποίο είναι δομημένος ένας κώδικας γλωσσικής επικοινωνίας.

Δεν πρέπει να ξεχνάμε ότι μια γλώσσα πρέπει να είναι καλή τόσο στην μετάδοση του προφορικού όσο και του γραπτού λόγου.

Οι "ανάγκες" πολλές φορές επιβάλλουν να επινοήσουμε άλλους τρόπους (κώδικες) επικοινωνίας. Όταν λέμε οι ανάγκες, ο καθένας μπορεί να φαντασθεί ό,τι θέλει. Από το ότι δεν θέλουμε ένα μήνυμα να γίνει γνωστό σε τρίτους, έως τα μέσα μετάδοσης που έχουμε στη διάθεσή μας. Για παράδειγμα, οι Ινδιάνοι χρησιμοποιούσαν σήματα καπνού. Σήμερα διαθέτουμε σύγχρονα ηλεκτομαγνητικά μέσα εγγραφής, αποθήκευσης και μετάδοσης μηνυμάτων. Ενδιάμεσα, όπου είχαμε στη διάθεσή μας τη στοιχειώδη χρήση του ηλεκτρικού ρεύματος, αρκούμαστε να αναφέρουμε την επινόηση και χρήση του κώδικα Morse.

Τα προηγούμενα αποτελούν μια αχλή ιδέα για το τι σημαίνει κώδικας επικοινωνίας. Στην αμέσως επόμενη παράγραφο θα προσπαθήσουμε να γίνουμε πιό συγκεκριμένοι.

1.2 Ορισμοί και στοιχειώδεις ιδιότητες

Έστω $\mathbb{A} = \{ a_1, a_2, \ldots, a_r \}$ ένα τυχαίο μη κενό πεπερασμένο σύνολο. Το σύνολο $\mathbb{A}$ θα το ονομάζουμε **αλφάβητο** , τα δε στοιχεία του **γράμματα** ή **χαρακτήρες** .

Μια πεπερασμένη ακολουθία χαρακτήρων από το αλφάβητο $\mathbb{A}$ θα ονομάζεται **στοιχειοσειρά** ή **λέξη** . Μια λέξη συνήθως θα τη συμβολίζουμε με ένα έντονο γράμμα του λατινικού αλφαβήτου.

Παράδειγμα 1.2.1. Έστω $\mathbb{A} = \{2, a, d, \diamond\}$, τότε τα $\mathbf{a} = a2d2aa$, $\mathbf{b} = d\diamond 2$, $\mathbf{c} = a$ είναι μερικές λέξεις που σχηματίζονται με χαρακτήρες από το αλφάβητο $\mathbb{A}$.

Το σύνολο όλων των λέξεων που μπορούμε να σχηματίσουμε με τους χαρακτήρες από ένα αλφάβητο $\mathbb{A}$ είναι άπειρο (γιατί;) και συμβολίζεται με $\mathbb{A}^*$.

Το πλήθος των χαρακτήρων σε μια λέξη $\mathbf{u} \in \mathbb{A}^*$ ονομάζεται **μήκος** και συμβολίζεται με $\ell(\mathbf{u})$. Στο προηγούμενο παράδειγμα οι λέξεις κατά σειρά έχουν μήκη $\ell(\mathbf{a}) = 6$, $\ell(\mathbf{b}) = 3$ και $\ell(\mathbf{u}) = 1$ αντίστοιχα.

Κάνουμε την παραδοχή ότι στο σύνολο $\mathbb{A}^*$ ανήκει και η *κενή* λέξη, δηλαδή η λέξη που δεν περιέχει κανένα χαρακτήρα, η οποία συνήθως συμβολίζεται με θ. Το μήκος της κενής λέξης προφανώς ισούται με μηδέν ($\ell(\theta) = 0$).

Έστω $\mathbf{u}, \mathbf{v} \in \mathbb{A}^*$ δύο λέξεις, τότε με την **παράθεση uv** των δύο λέξεων τη μια δίπλα στην άλλη σχηματίζεται μια άλλη λέξη $\mathbf{z} = \mathbf{uv} \in \mathbb{A}^*$. Προφανώς $\ell(\mathbf{z}) = \ell(\mathbf{u}) + \ell(\mathbf{v})$.

Έστω n ένας φυσικός αριθμός, με $\mathbb{A}^n$ θα συμβολίζουμε το σύνολο όλων των λέξεων με χαρακτήρες από το αλφάβητο $\mathbb{A}$, οι οποίες έχουν μήκος n. Προφανώς, επειδή το $\mathbb{A}$ είναι πεπερασμένο, το σύνολο $\mathbb{A}^n$ είναι πεπερασμένο. Μάλιστα ισχύει $|\,\mathbb{A}^n\,| = |\,\mathbb{A}\,|^n$ (γιατί;)

Πολλές φορές, όταν αναφερόμαστε (μόνο) στα στοιχεία του $\mathbb{A}^n$, αντί για λέξεις τα ονομάζουμε **διανύσματα**.

Ορισμός 1.2.2. *Έστω* $\mathbf{x} = a_1a_2\cdots a_n$, $\mathbf{y} = b_1b_2\cdots b_n \in \mathbb{A}^n$, *ορίζουμε την απεικόνιση* $d : \mathbb{A}^n \times \mathbb{A}^n \longrightarrow \mathbb{Z}$ *ως εξής*

$$d(\mathbf{x}, \mathbf{y}) = \sum_{i=1}^{n} r_i, \quad \text{όπου } r_i = \begin{cases} 0 & \text{αν } a_i = b_i \\ 1 & \text{αν } a_i \neq b_i \end{cases} .$$

Ο (μη αρνητικός) ακέραιος αριθμός $d(\mathbf{x}, \mathbf{y})$ *ονομάζεται* **(Hamming) απόσταση** *των δύο λέξεων* $\mathbf{x}$ *και* $\mathbf{y}$.

Δηλαδή η απόσταση $d(\mathbf{x}, \mathbf{y})$ παριστά το πλήθος των θέσεων στις οποίες οι δύο λέξεις $\mathbf{x}$ και $\mathbf{y}$ διαφέρουν.

Για παράδειγμα για τις λέξεις $\mathbf{a} = 2df3g4$ και $\mathbf{b} = 35fh24$ η μεταξύ τους απόσταση είναι ίση με 4.

(Προφανώς η απόσταση δύο λέξεων δεν υπερβαίνει το (κοινό) μήκος τους.)

Θεώρημα 1.2.3. *Η απεικόνιση* d *είναι μια μετρική στο σύνολο* $\mathbb{A}^n$, *δηλαδή για* $\mathbf{x}, \mathbf{y}$ *και* $\mathbf{z} \in \mathbb{A}^n$ *ισχύει.*

1. $d(\mathbf{x}, \mathbf{y}) \geq 0$, *με* $d(\mathbf{x}, \mathbf{y}) = 0$ *αν και μόνο αν* $\mathbf{x} = \mathbf{y}$.

2. $d(\mathbf{x}, \mathbf{y}) = d(\mathbf{y}, \mathbf{x})$.

3. $d(\mathbf{x}, \mathbf{z}) \leq d(\mathbf{x}, \mathbf{y}) + d(\mathbf{y}, \mathbf{z})$.

Απόδειξη. Η απόδειξη είναι αμέση συνέπεια του ορισμού και αφίνεται ως άσκηση. □

Παρατήρηση 1.2.4. Όλοι έχουμε υπ' όψη τη γνωστή Ευκλείδεια απόσταση στο χώρο $\mathbb{R}^n$, όπου $\mathbb{R}$ είναι το σύνολο των πραγματικών αριθμών.

Εδώ η έννοια της απόστασης που ορίσαμε προηγουμένως είναι θεμελιώδης για τα επόμενα, όπου, επιλέγοντας κατάλληλο αλφάβητο $\mathbb{A}$, μπορούμε να κάνουμε αντίστοιχη *Γεωμετρία*.

Ορισμός 1.2.5. *Έστω $\mathbb{A}$ ένα αλφάβητο. Κάθε μη κενό υποσύνολο $\mathcal{C}$ του $\mathbb{A}^*$ ονομάζεται* **κώδικας** *επί του αλφαβήτου $\mathbb{A}$ και τα στοιχεία του* **(κωδικο)λέξεις**.

(Πολλές φορές, όταν δεν υπάρχει το ενδεχόμενο σύγχυσης, τα στοιχεία ενός κώδικα τα αναφέρουμε και αυτά ως λέξεις, αντί για (κωδικο)λέξεις.)

Ο ορισμός που μόλις δώδαμε είναι απλούστατος στη διατύπωσή του, αλλά πολύ γενικός. Στα επόμενα θα δούμε τί περιορισμοί τίθενται στην επιλογή ενός *κατάλληλου* κώδικα.

Ας αρχίσουμε με την επιλογή του αλφαβήτου. Θεωρητικά κάθε πεπερασμένο μη κενό σύνολο μπορεί να θεωρηθεί ως αλφάβητο. Για μια όμως συστηματική μελέτη και ενασχόληση με τους κώδικες " επιβάλλεται " η επιλογή του αλφαβήτου να μην είναι τυχαία. Συνήθως επιλέγουμε ως αλφάβητο το $\mathbb{Z}_p$, τους ακεραίους $\mathrm{mod(p)}$, όπου p είναι ένας πρώτος αριθμός. Το $\mathbb{Z}_p$ είναι ένα σώμα ως προς την πρόσθεση και τον πολλαπλασιασμό (γενικώτερα θα μπορούσαμε να επιλέξουμε ως αλφάβητο ένα (τυχαίο) πεπερασμένο σώμα). Η επιλογή αυτή μας δίνει το πλεονέκτημα να χρησιμοποιήσουμε τις γνώσεις μας απο τα Μαθηματικά για την κατασκευή "καλών " κωδίκων.

(Το τι σημαίνει καλός κώδικας θα μας δοθεί η ευκαιρία να το διευκρινίσουμε στα επόμενα).

Ένας κώδικας επί του αλφαβήτου $\mathbb{Z}_2$ ονομάζεται **δυαδικός** κώδικας και γενικά επί του $\mathbb{Z}_p$ ονομάζεται **p-αδικός** κώδικας .

1.2.1 Κωδικοποίηση - Αποκωδικοποιήση

Άμεσα συνδεδεμένη με έναν κώδικα είναι η διαδικασία της κωδικοποίησης και αποκωδικοποίησης.

Έστω $S = \{ a_1, a_2, \ldots, a_s \}$ ένα πεπερασμένο σύνολο το οποίο ονομάζουμε **πηγή** και $\mathcal{C}$ ένας κώδικας, μια συνάρτηση **κωδικοποίησης** είναι μια συνάρτηση $f : S \longrightarrow \mathcal{C}$ η οποία είναι 1-1 και επί.

Η διαδικασία **κωδικοποίησης** συνίσταται, εφόσον είναι γνωστά τα σύνολα S και $\mathcal{C}$, στην επιλογή και εφαρμογή της συνάρτησης f.

Παραδείγματα 1.2.6. 1. Έστω ως πηγή $S = \{\alpha, \beta, \gamma, \ldots, \psi, \omega\}$, το σύνολο των γραμμάτων του Ελληνικού αλφαβήτου και ως κώδικας $\mathcal{C} = \{00, 01, \ldots, 23\}$, το σύνολο των διψηφίων αριθμών από το 00 έως και το 23. Μια συνάρτηση κωδικοποίησης είναι η $f(\alpha) = 00$, $f(\beta) = 01$, $f(\gamma) = 02, \ldots, f(\psi) = 22$, $f(\omega) = 23$.

Για παράδειγμα το "πηγαίο μήνυμα" *αγαπη* θα κωδικοποιηθεί ως 0002001607.

2. Ο κώδικας ASCII $\mathcal{C}$ είναι ένας δυαδικός κώδικας που περιλαμβάνει όλους τους αριθμούς από το 0 έως και το 127, αλλά εκφρασμένους ως επταψήφιους αριθμούς στο δυαδικό σύστημα. Δηλαδή $\mathcal{C} = \mathbb{Z}_2^7$. Η πηγή αποτελείται από όλα τα γράμματα του Λατινικού αλφαβήτου (κεφαλαία και πεζά), από τα σημεία στήξης, καθώς επίσης και από διάφορους χαρακτήρες ελέγχου (σύνολον 128 χαρακτήρες). Υπάρχει μια συνάρτηση η οποία κωδικοποιεί κάθε ένα από τους 128 χαρακτήρες σε έναν επταψήφιο δυαδικό αριθμό. Στον επόμενο πίνακα παρουσιάζεται (μερικώς) η κωδικοποίηση του Λατινικού αλφαβήτου στον δυαδικό κώδικα ASCII.

$A \to 1000001$	$J \to 1001010$	$S \to 1010011$
$B \to 1000010$	$K \to 1001011$	$T \to 1010100$
$C \to 1000011$	$L \to 1001100$	$U \to 1010101$
$D \to 1000100$	$M \to 1001101$	$V \to 1010110$
$E \to 1000101$	$N \to 1001110$	$W \to 1010111$
$F \to 1000110$	$O \to 1001111$	$X \to 1011000$
$G \to 1000111$	$P \to 1010000$	$Y \to 1011001$
$H \to 1001000$	$Q \to 1010001$	$Z \to 1011010$
$I \to 1001001$	$R \to 1010010$	$Space \to 0100000$

Η **αποκωδικοποίηση** συνίσταται στην αντίστροφη διαδικασία. Επειδή η συνάρτηση κωδικοποίησης, έστω f, είναι 1-1 και επί υπάρχει η αντίστροφή της f^{-1}. Οπότε όταν έχουμε μια (κωδικο)λέξη, δεν έχουμε παρά να εφαρμόσουμε την f^{-1} και να βρούμε το στοιχείο της πηγής στο οποίο αντιστοιχεί η δοθείσα (κωδικο)λέξη.

Για παράδειγμα το κωδικοποιημένο, στον κώδικα ASCII, μήνυμα 1001100100111110101101000110 αποκωδικοποιείται, με τη βοήθεια του πίνακα, ως LOVE.

Παρατήρηση 1.2.7. Η απαίτηση η συνάρτηση κωδικοποίησης να είναι 1 - 1 και επί είναι πολύ σημαντική, καθότι μόνο τότε η αποκωδικοποίηση μπορεί να είναι αποτελεσματική. Ας δούμε το εξής απλό παράδειγμα. Υποθέτουμε ότι έχουμε το σύνολο των ακεραίων αριθμών ως πηγή και το ίδιο σύνολο ως κώδικα και ότι "κωδικοποιούμε" κάθε ακέραιο αριθμό με το τετράγωνό του. Δηλαδή έχουμε την συνάρτηση $f : \mathbb{Z} \longrightarrow \mathbb{Z}$ με $f(x) = x^2$. Τότε, αν πάρουμε τον αριθμό 4 ως (κωδικο)λέξη, επειδή η f δεν είναι 1 - 1, κατά την "αποκωδικοποίηση" έχουμε πρόβλημα καθότι δεν γνωρίζουμε αν το "πηγαίο μήνυμα " ήταν το 2 ή το -2. Επίσης, επειδή η f δεν είναι επί, υπάρχουν (κωδικο)λέξεις οι οποίες δεν είναι εικόνα (μέσω της f) κανενός στοιχείου της πηγής, οπότε αυτές οι λέξεις "περιττεύουν ".

Δεν αρκεί όμως μόνο η απαίτηση η συνάρτηση κωδικοποίησης να είναι 1 - 1 και επί. Ας επανέλθουμε στα προηγούμενα παραδείγματα.

Στο πρώτο παράδειγμα, υποθέτουμε ότι ο κώδικας μας δεν είναι ο $\mathcal{C} = \{00, 01, \ldots, 23\}$, αλλά ο $\bar{\mathcal{C}} = \{0, 1, \ldots, 23\}$. Αν συνάρτηση κωδικοποίησης είναι η $\bar{f}(\alpha) = 0$, $\bar{f}(\beta) = 1$, $\bar{f}(\gamma) = 2, \ldots, \bar{f}(\psi) = 22$, $\bar{f}(\omega) = 23$, τότε η ακολουθία χαρακτήρων 0002001607 θα μπορούσε να προέρχεται από περισσότερα του ενός "πηγαία μηνύματα ". Πράγματι ενδέχεται να έχουμε *αααγααβηαθ*, αλλά και *αααφαραθ ή αααφαβηαθ*. Το πρόβλημα που προκύπτει στην περίπτωση αυτή οφείλεται στο γεγονός ότι οι (κωδικο)λέξεις στον κώδικα $\bar{\mathcal{C}}$ δεν έχουν όλες το ίδιο μήκος.

Στο δεύτερο παράδειγμα οι κωδικολέξεις έχουν όλες μήκος 7. Εδώ όμως το γράμμα Ε, που χρησιμοποιείται συχνότατα, "απαιτεί" τον ίδιο χρόνο και χώρο, για να κωδικοποιηθεί, με το γράμμα Q, που συναντάται σπανιώτατα.

Ορισμός 1.2.8. *Ένας κώδικας $\mathcal{C}$ ονομάζεται κώδικας* **σταθερού μήκους** *αν όλες οι (κωδικο)λέξεις έχουν το ίδιο μήκος, δηλαδή υπάρχει ένας θετικός ακέραιος αριθμός n έτσι ώστε $\mathcal{C} \subseteq \mathbb{A}^n$, ο αριθμός n ονομάζεται* **μήκος** *του κώδικα . Διαφορετικά ο κώδικας ονομάζεται* **μεταβλητού μήκους**.

Ανάλογα με το αν ένας κώδικας είναι σταθερού ή μεταβλητού μήκους, όπως έχουμε επισημάνει, παρουσιάζει πλεονεκτήματα και μειονεκτήματα. Στα επόμενα εμείς θα ασχοληθούμε κυρίως με **p**-αδικούς κώδικες σταθερού μήκους. Επομένως ένας κώδικας θα χαρακτηρίζεται, προς το παρόν από τις παραμέτρους: Το αλφάβητο, το μήκος n και το μέγεθος του $M = \mid \mathcal{C} \mid$. Μάλιστα για συντομία θα αναφέρεται ως ένας **p**-αδικός (n, M) κώδικας.

Ένα άμεσο πλεονέκτημα της χρήσης **p**-αδικών κωδίκων σταθερού μήκους είναι ότι το σύνολο $\mathbb{Z}_p^n$ όλων των λέξεων μήκους n είναι διανυσματικός χώρος, επομένως μπορούμε να χρησιμοποιήσουμε τις ιδιότητες ενός διανυσματικού χώρου στη μελέτη των κωδίκων. Προς το παρόν αναφέρουμε έναν ορισμό και μια πρόταση πολύ σημαντική για τα επόμενα.

Ορισμός 1.2.9. *Έστω* $\mathbf{a} \in \mathbb{A}^n$ *(* $\mathbb{A} = \mathbb{Z}_p$ *). Η απόσταση της* $\mathbf{a}$ *από τη μηδενική λέξη* $\mathbf{0} = (0, 0, \ldots, 0)$ *ονομάζεται* **βάρος** *της* $\mathbf{a}$ *και συμβολίζεται με* $w(\mathbf{a})$*. Δηλαδή* $w(\mathbf{a}) = d(\mathbf{a}, \mathbf{0})$*.*

Διαφορετικά, το βάρος μιας λέξης παριστά τον αριθμό των μη μηδενικών χαρακτήρων της.

Στην περίπτωση ένος δυαδικού κώδικα ορίζεται η **τομή** δύο (κωδικο)λέξεων $\mathbf{a} = (a_1, a_2, \ldots, a_n)$, $\mathbf{b} = (b_1, b_2, \ldots, b_n) \in \mathbb{Z}_2^n$ ως εξής:
$\mathbf{a} \cap \mathbf{b} = (a_1 b_1, a_2 b_2, \ldots, a_n b_n)$. Δηλαδή η λέξη $\mathbf{a} \cap \mathbf{b}$ έχει 1 σε μια θέση αν και μόνο αν και η $\mathbf{a}$ και η $\mathbf{b}$ έχουν 1 στην αντίστοιχη θέση.

Πρόταση 1.2.10. *1. Για* $\mathbf{a}, \mathbf{b}, \mathbf{c} \in \mathbb{Z}_p^n$ *ισχύει.*

(α΄) $d(\mathbf{a}, \mathbf{b}) = w(\mathbf{a} - \mathbf{b})$.

(β΄) $d(\mathbf{a} + \mathbf{c}, \mathbf{b} + \mathbf{c}) = d(\mathbf{a}, \mathbf{b})$.

2. Στην περίπτωση όπου $\mathbf{a}, \mathbf{b} \in \mathbb{Z}_2^n$*, τότε* $d(\mathbf{a}, \mathbf{b}) = w(\mathbf{a} + \mathbf{b}) = w(\mathbf{a}) + w(\mathbf{b}) - 2w(\mathbf{a} \cap \mathbf{b})$.

Όπου οι πράξεις της πρόσθεσης και αφαίρεσης είναι οι γνωστές πράξεις κατά συντεταγμένες στον διανυσματικό χώρο $\mathbb{Z}_p^n$*.*

Απόδειξη. Η απόδειξη είναι άμεση συνέπεια του ορισμού και αφίνεται ως άσκηση. □

Κατά την κωδικοποίηση ενός (πηγαίου) μηνύματος, όπως έχουμε πει, εφαρμόζεται η συνάρτηση κωδικοποίησης. Κατόπιν το κωδικοποιημένο μήνυμα αποστέλλεται κάπου, χρησιμοποιώντας γραμμές τηλεφώνου, ηλεκτομαγνητικά κύμματα κ.λ.π.. Επίσης μπορεί να αποθηκευθεί σε μαγνητοταινίες, σε δίσκους ακτίνας, στη μνήμη ενός υπολογιστή κ.λ.π.. Για την αποκωδικοποιήση ακολουθείται η αντίστροφη διαδικασία, δηλαδή εφαρμόζεται η αντίστροφη συνάρτηση της συνάρτησης κωδικοποίησης.

Σε ιδανικές περιπτώσεις δεν θα είχαμε **κανένα** πρόβλημα. Αρκούσε ο **αποστολέας** να γνωρίζει τον "τύπο" της συνάρτησης κωδικοποίησης και ο **παραλήπτης** [1] να γνωρίζει τον "τύπο" της αντίστροφης συνάρτησης. Στην πραγματικότητα όμως η κατάσταση είναι τελείως διαφορετική. Κατά τη "διαχείριση" του κωδικοποιημένου μηνύματος (αποστολή, αποθήκευση κ.λ.π.) επέρχονται αλλοιώσεις στις (κωδικο)λέξεις, [2] οπότε η εφαρμογή της αντίστροφης συνάρτησης

[1] Οι λέξεις αποστολέας και παραλήπτης θα χρησιμοποιούνται με την ευρεία έννοια του όρου είτε πρόκειται για πρόσωπα, είτε πρόκειται για μηχανές.

[2] Εδώ δεν θα ασχοληθούμε με τα αίτια που προκαλούν τις αλλοιώσεις, είτε αυτές είναι σκόπιμες, είτε οφείλονται σε τεχνικές ατέλειες κ.λ.π.

κωδικοποίησης όχι μόνο δεν προσφέρει, αλλά μπορεί να οδηγήσει σε "στρεβλώσεις".

Ένας από τους κύριους σκοπούς της Θεωρίας Κωδικών είναι η αντιμετώπιση τέτοιων καταστάσεων. Στην επόμενη παράγραφο θα προσπαθήσουμε να αντιμετωπίσουμε αυτό το πρόβλημα πιο συστηματικά. Προς το παρόν αρκούμαστε να δώσουμε δύο παραδείγματα (πραγματικών) προβλημάτων.

1. Κατά τις πρώτες αποστολές διαστημοπλοίων στο διάστημα για να μεταδοθούν οι (ασπρόμαυρες) φωτογραφίες των πλανητών στη γη είχε επινοηθεί η εξής απλή, αλλά πολύ εφυής στη σύλληψή της, μέθοδος. Κάθε φωτογραφία χωρίζονταν σε μικρότερα τετράγωνα (π.χ. σε m γραμμές επί n στήλες), οι διάφορες αποχρώσεις του γκρίζου χρώματος κατατάχθηκαν σε 64 διαβαθμίσεις (από το 0 για το άσπρο έως το 63 για το μαύρο). Κάθε αριθμός μετατράπει στην αντίστοιχη δυαδική έκφραση ($0 = 000000, 1 = 000001, \ldots, 63 = 111111$), [3] οπότε για τη μετάδοση της φωτογραφίας εγίνετο (με προκαθορισμένη σειρά) μια σάρωση των επιμέρους τετραγώνων και ανάλογα με το βαθμό αμαυρώσεως απεστέλετο η αντίστοιχη εξάδα των 0 και 1. Οι αποδέκτες στη γη δεν είχαν παρά, ανάλογα με την εξάδα που ελαμβάνετο, να βρούν την αντίστοιχη απόχρωση του γκρίζου και να αναπαράγουν τη φωτογραφία σύμφωνα με την προκαθορισμένη σειρά σάρωσης.

Όλα αυτά θα συνέβαιναν στην ιδανική περίπτωση όπου δεν θα επέρχονταν αλλοιώσεις κατά τη μετάδοση των εξάδων. Αρκούσε όμως η αλλαγή ενός χαρακτήρα από 0 σε 1 (και αντίστροφα) οπότε η εξάδα αντιστοιχούσε σε διαφορετική απόχρωση με αποτέλεσμα να μην έχουμε πιστή αναπαραγωγή της φωτογραφίας.

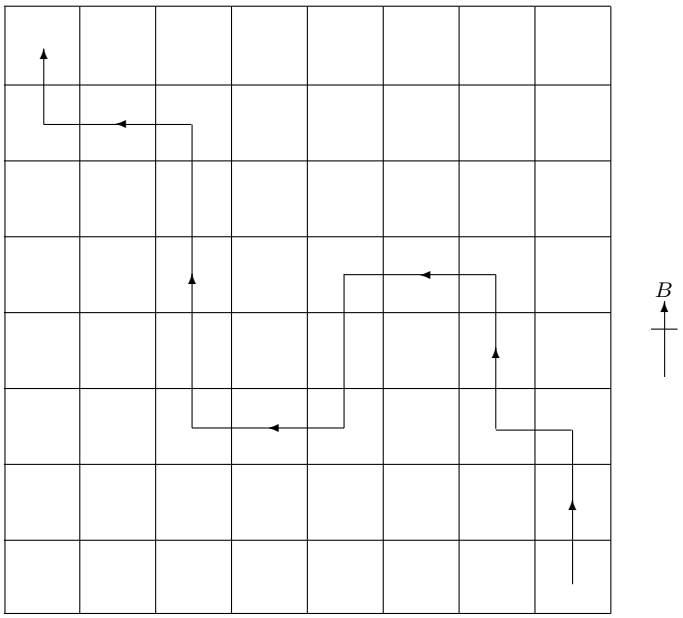
Το πρόβλημα αυτό αντιμετωπίστικε ως εξής· Οι 64 εξάδες κωδικοποιήθηκαν σε (κωδικο)λέξεις μήκους 32, οι οποίες αποτελούνταν από 0 και 1, κατά τέτοιο τρόπο ώστε όταν απεστέλετο μια 32-άδα, θα μπορούσε να επέλθει αλλοίωση (μέχρι και) σε επτά το πλήθος χαρακτήρες, αλλά να αποδίδεται σωστά η πραγματική απόχρωση. (Στα επόμενα, δες στη σελίδα 149, θα μας δοθεί η ευκαιρία να δούμε πως έγινε αυτή η κωδικοποίηση). Βέβαια δεν πρέπει να ξεχνάμε το "κόστος" αυτής της κωδικοποίησης το οποίο μεταφράζεται σε χρόνο μετάδοσης και σε απαίτηση μνήμης.

2. Υποθέτουμε ότι ένα πλοίο θέλει να διελεύσει ανάμεσα σε επικίνδυνες ακτές και ζητά τη βοήθεια των τοπικών λιμενικών αρχών. Ο κυβερνήτης και ο λιμενάρχης έχουν ακριβώς ίδιους χάρτες της περιοχής, αλλά η ασφαλής πορεία είναι χαραγμένη μόνο στο χάρτη του λιμενάρχη, ο οποίος αναλαμβάνει να δώσει οδηγίες. Επειδή δεν είναι δυνατόν να δίνονται φωνητικές οδηγίες της μορφής "...πήγαινε προς Βορράν, μετά προς Δυσμάς ...". Ο τρόπος επικοινωνίας γίνεται

[3] Η ίδια ιδέα εφαρμόζεται και σήμερα στις ψηφιακές φωτογραφίες, μόνο που τώρα (για να πετύχουμε υψηλή πιστότητα και ευκρίνεια) δεν χρησιμοποιούμε 64 αποχρώσεις του γκρίζου αλλά τουλάχιστον $2^{16} = 65536$ αποχρώσεις όλων των χρωμάτων.

μέσω ενός μέσου, όπου μπορούν να μεταδοθούν μόνο τα σύμβολα 0 και 1. Τότε έχουμε μια πηγή $S = \{\,\mathbf{A}\text{νατολή}, \mathbf{\Delta}\text{ύση}, \mathbf{B}\text{ορράς}, \mathbf{N}\text{ότος}\,\}$, έναν κώδικα $\mathcal{C} = \{\,00, 01, 10, 11\,\}$ και μια συνάρτηση κωδικοποίησης $f : S \longrightarrow \mathcal{C}$ με $f(\mathbf{A}) = 00$, $f(\mathbf{\Delta}) = 01$, $f(\mathbf{B}) = 10$, $f(\mathbf{N}) = 11$. Ο κώδικας αυτός είναι ο μικρότερος δυνατόν, καθότι για την μετάδοση ενός στοιχείου από την πηγή S αρκούν δύο χαρακτήρες. Κατά συνέπεια είναι "γρήγορος και οικονομικός".

Ο λιμενάρχης για να περιγράψει τη χαραγμένη πορεία (βλέπε σχήμα) πρέπει να μεταδόσει κωδικοποιημένο το εξής (πηγαίο) μήνυμα BBΔBBΔΔNNΔΔBBB-BΔΔB. Δηλαδή μεταδίδει το μήνυμα 10 10 01 10 ..... . Ο κυβερνήτης δεν έχει παρά να αποκωδικοποιήσει το μήνυμα που λαμβάνει εφαρμόζοντας την αντίστροφη συνάρτηση f^{-1} και να πορευθεί αναλόγως.



Σε ιδανικές συνθήκες μετάδοσης/λήψης δεν υπάρχει πρόβλημα. Στην πράξη όμως η αλλαγή ενός χαρακτήρα από 0 σε 1 (και αντίστροφα) μπορεί να οδηγήσει σε λάθος πορεία και να εκθέσει σε κίνδυνο το πλοίο. Επειδή η ασφάλεια προέχει, πρέπει να επινοηθεί ένας άλλος "ασφαλέστερος" κώδικας, ακόμα και αν είναι πιο "απαιτητικός " σε χρόνο και μνήμη.

Υποθέτουμε ότι αντί του κώδικα $\mathcal{C}$ έχουμε τον κώδικα
$\mathcal{D} = \{\,000, 011, 101, 110\,\}$ και συνάρτηση κωδικοποίησης $g : S \longrightarrow \mathcal{D}$ με $g(\mathbf{A}) = 000$, $g(\mathbf{\Delta}) = 011$, $g(\mathbf{B}) = 101$, $g(\mathbf{N}) = 110$. Παρατηρούμε ότι ο κώδικας $\mathcal{D}$ προέρχεται από τον προηγούμενο κώδικα επισυνάπτοντας ένα επιπλέον

ψηφίο με τέτοιο τρόπο ώστε ο αριθμός των 1 που εμφανίζονται σε κάθε (κωδικο)λέξη να είναι πάντα άρτιος. Αν κατά τη μετάδοση μιας τριάδας χαρακτήρων (μιας (κωδικο)λέξης) επέλθει "αλλοίωση" ενός χαρακτήρα , τότε η τριάδα που λαμβάνει ο κυβερνήτης του πλοίου δεν αντιστοιχεί σε καμία (κωδικο)λέξη (γιατί;) και αντιλαμβάνεται ότι πρόκειται περί λάθους. Δηλαδή έχει "ανιχνευθεί" λάθος, οπότε (αν υπάρχει δυνατότητα) ζητά την επανάληψη της αποστολής της συγκεκριμένης (κωδικο)λέξης.

Πολλές φορές όμως δεν είναι δυνατή η επικοινωνία του κυβερνήτη (παραλήπτη) με τον λιμενάρχη (αποστολέα) για να ζητηθούν διευκρινίσεις. [4] Τότε είναι αναγκαίο να "επιστρατευθεί" ένας κώδικας ο οποίος να είναι περισσότερο "αποτελεσματικός ". Θα δούμε πώς αντιμετωπίζεται αυτό το πρόβλημα στα επόμενα (βλέπε Παράδειγμα $1.3.8_2$).

1.2.2 Το πρόβλημα της αποκωδικοποίησης

Έστω ότι επικοινωνούμε μέσω ενός $p-$αδικού κώδικα $\mathcal{C} \subseteq \mathbb{A}^n$ $(\mathbb{A} = \mathbb{Z}_p)$. Όταν αποστέλεται μία (κωδικο)λέξη, έστω $\mathbf{a}$, ενδέχεται, όπως έχουμε προείπει, να λάβουμε μια άλλη λέξη $\mathbf{b}$. Η *διαφορά* $\mathbf{e} = \mathbf{b} - \mathbf{a} \in \mathbb{A}^n$ [5] λέγεται **διάνυσμα λάθους** ή απλώς **λάθος** που παρέσφυσε (υπεισήλθε) κατά τη μετάδοση.

(Ορισμένες φορές τα λάθη αναφέρονται ως **παράσιτα** ή ως **θόρυβοι**.)

Για παράδειγμα, σε ένα 5-δικό κώδικα μήκους 4, αν εστάλει η λέξη $\mathbf{a} = 2034$ και ελήφθει η λέξη $\mathbf{b} = 3021$, τότε το λάθος είναι $\mathbf{e} = 1042$. Όπως βλέπουμε, στις θέσεις του λάθους, όπου εμφανίζονται μη μηδενικές συντεταγμένες, στις αντίστοιχες θέσεις της αρχικής λέξης έχει επέλθει *αλλοίωση* του αντίστοιχου χαρακτήρα. Τις περισσότερες φορές δεν μας ενδιαφέρει τί είδους αλλοίωση έχει προκληθεί σε ένα χαρακτήρα, αλλά απλώς αν έχει ή δεν έχει επέλθει αλλοίωση ενός χαρακτήρα. Οπότε σαν λάθος εννοούμε ένα διάνυσμα $\varepsilon \in \mathbb{A}^n$, το οποίο έχει 1 στις θέσεις όπου έχει επέλθει αλλοίωση του χαρακτήρα και 0 στις υπόλοιπες θέσεις. Στο προηγούμενο παράδειγμα έχουμε $\varepsilon = 1011$.

Όπως παρατηρούμε $d(\mathbf{a}, \mathbf{b}) = w(\mathbf{e}) = w(\varepsilon)$. Επίσης αν ο κώδικας $\mathcal{C}$ είναι δυαδικός, τότε $\mathbf{e} = \varepsilon$ (γιατί;)

Το μεγάλο πρόβλημα στην αποκωδικοποίηση είναι η εύρεση μιας διαδικασίας, η οποία να αποφαίνεται, όταν λαμβάνεται μια λέξη, κατά πόσο αυτή η λέξη εμπεριέχει λάθη. Πολύ δε περισσότερο να αποφασίζει ποιά (κωδικο)λέξη εστάλει. Μια

[4] Η περίπτωση μη δυνατότητας επικοινωνίας παραλήπτη με αποστολέα είναι η πιο συνήθης. Για παράδειγμα, είναι δύσκολο να ζητηθεί η επανάληψη της αποστολής μιας φωτογραφίας από το διάστημα. Όπως είναι αδύνατον, όταν θέλουμε να αναπαράγουμε το αποθηκευμένο υλικό μιας μαγνητοταινίας, να ζητήσουμε την επαναποθήκευσή του, όταν παρουσιάζονται προβλήματα σωστής αναπαργωγής.

[5] Ως αλφάβητο $\mathbb{A}$ έχει επιλεγεί το σώμα $\mathbb{Z}_p$, οπότε η διαφορά ορίζεται ως αφαίρεση κατά συνταταγμένες

τέτοια διαδικασία προφανώς εξαρτάται, κατά κύριο λόγο, από το μέσον που χρησιμοποιείται για τη μετάδοση των μυνημάτων. Για παράδειγμα: Υποθέτουμε ότι έχουμε τον δυαδικό κώδικα $\mathcal{C} = \{\, 00000,\ 11111 \,\}$ και ότι λάβαμε τη λέξη 11100, τότε εφαρμόζοντας τη "λογική " ότι αυτή η λέξη είναι "πλησιέστερα " προς την (κωδικο)λέξη 11111 δεχόμαστε ότι η λέξη που εστάλει είναι η λέξη 11111. Αν όμως κάνουμε την παραδοχή ότι το μέσον μετάδοσης που διαθέτουμε αλλοιώνει πάντα τον πρώτο χαρακτήρα κάθε λέξης που στέλνεται, τότε η λέξη 11100 που λάβαμε είναι "πλησιέστερα " προς την (κωδικο)λέξη 00000. Επίσης ενδέχεται σε διαφορετικές χρονικές στιγμές να έχουμε διαφορετικό τρόπο μετάδοσης του ιδίου χαρακτήρα. Επομένως η φύση του μέσου μετάδοσης καθορίζει κατά κύριο λόγο τον "κανόνα αποφασισιμότητας" με τον οποίο κάνουμε την αποκωδικοποίηση. Ας γίνουμε πιο συγκεκριμένοι.

Ορισμός 1.2.11. *Ένας* **δίαυλος επικοινωνίας** *αποτελείται από ένα αλφάβητο* $\mathbb{A} = \{\, a_1, a_2, \ldots, a_r \,\}$*, το ίδιο με το αλφάβητο του κώδικα, και ένα σύνολο πιθανοτήτων* $p_{ij} = p(\epsilon\lambda\acute{\eta}\varphi\theta\epsilon\iota\ o\ \chi\alpha\rho\alpha\kappa\tau\acute{\eta}\rho\alpha\varsigma\ a_i \mid \epsilon\sigma\tau\acute{\alpha}\lambda\epsilon\iota\ o\ \chi\alpha\rho\alpha\kappa\tau\acute{\eta}\rho\alpha\varsigma\ a_j)$*, το οποίο ικανοποιεί τη σχέση*

$$\sum_{i=1}^{r} p_{ij} = 1$$

για όλα τα j*.*

Οι πιθανότητες p_{ij} ονομάζονται **πιθανότητες μετάδοσης** .

Εδώ γίνεται η παραδοχή ότι οι πιθανότητες αυτές σε έναν δίαυλο επικοινωνίας δεν αλλάζουν από χρονική σε χρονική στιγμή.

Η προηγούμενη σχέση δηλώνει: Δεδομένου ότι εστάλει ένας χαρακτήρας, πάντα λαμβάνεται ένας χαρακτήρας. Επίσης παραδεχόμαστε ότι ποτέ δεν λαμβάνεται ένας χαρακτήρας αν δεν έχει σταλεί (κάποιος) χαρακτήρας. Δηλαδή ένας δίαυλος δεν αυξομειώνει το μήκος μιας ακολουθίας χαρακτήρων που αποστέλεται μέσω αυτού.

Ορισμός 1.2.12. *Ένας δίαυλος θα λέγεται* **αμνήμων** *αν η μετάδοση ενός χαρακτήρα είναι ανεξάρτητη από τη μετάδοση προηγουμένων χαρακτήρων.*

Η ιδιότητα αυτή με τη βοήθεια των πιθανοτήτων μετάδοσης μπορεί να περιγραφεί ως εξής: Έστω η (κωδικο)λέξη $\mathbf{c} = c_1\, c_2 \cdots c_n$ και η λέξη $\mathbf{x} = x_1\, x_2 \cdots x_n$. Τότε η πιθανότητα $p(\epsilon\lambda\acute{\eta}\varphi\theta\epsilon\iota\ \eta\ \lambda\acute{\epsilon}\xi\eta\ \mathbf{x} \mid \epsilon\sigma\tau\acute{\alpha}\lambda\epsilon\iota\ \eta\ \lambda\acute{\epsilon}\xi\eta\ \mathbf{c})$ είναι ίση με το γινόμενο των πιθανοτήτων μετάδοσης $p(\epsilon\lambda\acute{\eta}\varphi\theta\epsilon\iota\ o\ \chi\alpha\rho\alpha\kappa\tau\acute{\eta}\rho\alpha\varsigma\ x_i \mid \epsilon\sigma\tau\acute{\alpha}\lambda\epsilon\iota\ o\ \chi\alpha\rho\alpha\kappa\tau\acute{\eta}\rho\alpha\varsigma\ c_i)$. Δηλαδή

$$p(\,\epsilon\lambda\acute{\eta}\varphi\theta\epsilon\iota\ \eta\ \ \mathbf{x}\ \mid\ \ \epsilon\sigma\tau\acute{\alpha}\lambda\epsilon\iota\ \eta\ \mathbf{c}\,) = \prod_{i=1}^{n} p(\,\epsilon\lambda\acute{\eta}\varphi\theta\epsilon\iota\ o\ x_i\ \mid\ \epsilon\sigma\tau\acute{\alpha}\lambda\epsilon\iota\ o\ \ c_i) \quad (1.2.1)$$

Όπως καταλαβαίνουμε ένας "καλός" δίαυλος είναι ένας δίαυλος, όπου οι πιθανότητες μετάδοσης p_{ij} είναι "πολύ μικρές" για $i \neq j$ και "πολύ μεγάλες" για $i = j$. Στην ιδανική περίπτωση, όπου $p_{ij} = 0$ για $i \neq j$ (οπότε $p_{ii} = 1$) για όλα τα $i, j = 1, 2, \ldots, r$, έχουμε έναν **αθόρυβο** δίαυλο και δεν θα υπήρχε πρόβλημα αποκωδικοποίησης.

Τις περισσότερες φορές (χωρίς αυτό να συμβαίνει στην πραγματικότητα) υποτίθεται ότι όλες οι πιθανότητες μετάδοσης p_{ij} για όλα τα $i \neq j$ είναι ίσες μεταξύ τους, όπως επίσης όλες οι πιθανότητες p_{ii} για όλα τα i είναι ίσες μεταξύ τους. Οπότε, αν για έναν $r-$αδικό δίαυλο θα έχουμε $p_{ij} = p$, τότε $p_{ii} = 1 - (r-1)p$ (γιατί ;). Ένας τέτοιος δίαυλος θα λέγεται **συμμετρικός** .

Στην περίπτωση ενός δυαδικού κώδικα μήκους n, που οι (κωδικο)λέξεις μεταδίδονται μέσω ενός συμμετρικού δίαυλου επικοινωνίας, η πιθανότητα να αλλοιωθούν k το πλήθος χαρακτήρες είναι ίση με $p^k(1-p)^{n-k}$.

Παρατήρηση 1.2.13. Στον ορισμό ενός δίαυλου επικοινωνίας είχαμε δεχθεί ότι μεταξύ των πιθανοτήτων μετάδοσης ισχύει η σχέση

$$\sum_{i=1}^{r} p_{ij} = 1$$

για όλα τα j, η οποία δηλώνει, δεδομένου ότι εστάλει ένας χαρακτήρας, πάντα λαμβάνεται ένας χαρακτήρας.

Στην πράξη όμως δεν αποκλείεται το ενδεχόμενο, να έχει σταλεί ένας χαρακτήρας, αλλά κατά τη μετάδοση ο χαρακτήρας να *χαθεί* (προσοχή! εννοούμε απώλεια χαρακτήρα και όχι αλλοίωση). Στην περίπτωση αυτή θα είχαμε μείωση του μήκους της μεταδιδόμενης λέξης, κάτι που θα δημιουργούσε πρόσθετα προβλήματα.

Το ενδεχόμενο αυτό αντιμετωπίζεται (συνήθως) ως εξής: Ως αλφάβητο επικοινωνίας, άρα και αλφάβητο του κώδικα, χρησιμοποιείται το *διευρυμένο* αλφάβητο $\bar{\mathbb{A}} = \mathbb{A} \cup \{?\}$, όπου ο χαρακτήρας ? δεν αποστέλλεται ποτέ, αλλά εμφανίζεται στη θέση ένος απωλεσθέντος χαρακτήρα. Οπότε για τις πιθανότητες μετάδοσης έχουμε $p(\textit{ελήφθει ο χαρακτήρας } a_i \mid \textit{εστάλει ο χαρακτήρας } ?) = 0$, $p(\textit{ελήφθει ο χαρακτήρας } ? \mid \textit{εστάλει ο χαρακτήρας } a_j) \geq 0$. Επομένως για να ισχύει η παραπάνω σχέση αναγκαστικά έχουμε (γιατί;)
$p(\textit{ελήφθει ο χαρακτήρας } ? \mid \textit{εστάλει ο χαρακτήρας } ?) = 1$.

1.2.3 Ασκήσεις

1. Έστω $\mathbf{a} \in \mathbb{Z}_r^n$. Δείξτε ότι υπάρχουν $\binom{n}{k}(r-1)^k$ το πλήθος λέξεις του $\mathbb{Z}_r^n$, οι οποίες απέχουν απόσταση ίση με k από την $\mathbf{a}$.

2. *i)* Υποθέτουμε ότι θέλουμε έναν δυαδικό κώδικα σταθερού μήκους που να έχει 126 (κωδικο)λέξεις. Πιό είναι το μικρότερο δυνατό μήκος για έναν τέτοιο κώδικα;

   ii) Υποθέτουμε ότι θέλουμε έναν δυαδικό κώδικα σταθερού μήκους που να έχει n το πλήθος (κωδικο)λέξεις. Πιό είναι το μικρότερο δυνατό μήκος για έναν τέτοιο κώδικα;

3. Ποιές συναρτήσεις κωδικοποίησης μπορούμε να ορίσουμε από την πηγή $S = \{a, b, c\}$ στον κώδικα $\mathcal{C} = \{00, 01, 11\}$;

4. Να υπολογίσετε τον αριθμό των συναρτήσεων κωδικοποίησης από μια πηγή μεγέθους n σε έναν κώδικα μεγέθους n.

5. Να υπολογίσετε τον αριθμό των κωδίκων μήκους n που μπορούμε να ορίσουμε επί ενός αλφαβήτου μεγέθους m.

6. Υποθέτουμε ότι έχουμε έναν δυαδικό συμμετρικό δίαυλο επικοινωνίας με πιθανότητα μετάδοσης
   $p = p(\textit{ελήφθει ο χαρακτήρας } 0 \mid \textit{εστάλει ο χαρακτήρας } 1) =$
   $= p(\textit{ελήφθει ο χαρακτήρας } 1 \mid \textit{εστάλει ο χαρακτήρας } 0) > \frac{1}{2}$. Τί πρέπει να κάνουμε;

1.3 Κανόνες Αποκωδικοποίησης

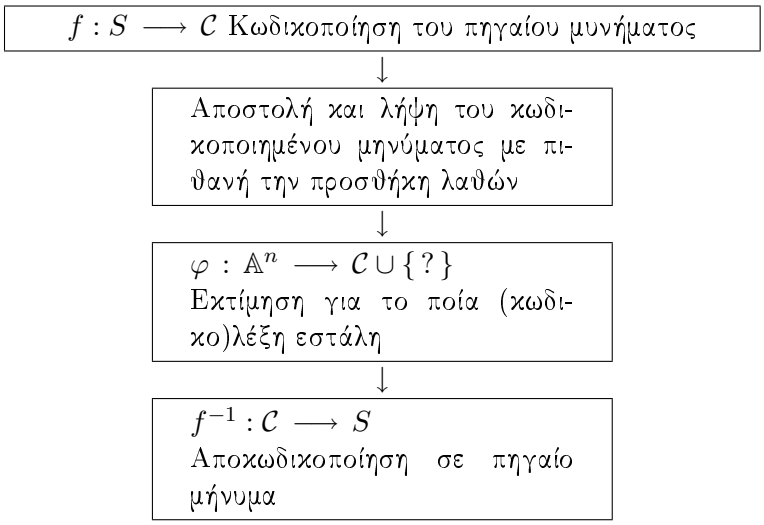
Όπως έχουμε επισημάνει στην προηγούμενη παράγραφο, το μεγάλο πρόβλημα στην αποκωδικοποίηση είναι η εύρεση μιας διαδικασίας, η οποία να αποφαίνεται, όταν λαμβάνεται μια λέξη, κατά πόσο αυτή η λέξη εμπεριέχει λάθη. Πολύ δε περισσότερο να αποφασίζει ποιά λέξη εστάλει.

Στην παράγραφο αυτή θα δούμε πώς αντιμετωπίζεται το πρόβλημα της αποκωδικοποίησης εφαρμόζοντας κάποιους *κανόνες αποφασισιμότητας*.

Ορισμός 1.3.1. *Έστω ένας κώδικας $\mathcal{C}$ μήκους n με χαρακτήρες από το αλφάβητο $\mathbb{A}$ ένας κανόνας* **αποφασισιμότητας** *είναι μια συνάρτηση*
$\varphi : \mathbb{A}^n \longrightarrow \mathcal{C} \cup \{?\}$. *Η οποία* αποδέχεται *τη λέξη $\mathbf{x} \in \mathbb{A}^n$ ως τη λέξη $\varphi(\mathbf{x})$ αν $\varphi(\mathbf{x}) \in \mathcal{C}$ ή αποφαίνεται ότι πρόκειται για λάθος αν $\varphi(\mathbf{x}) = ?$.*

Εδώ πρέπει να επισημάνουμε ότι η συνάρτηση φ, που μόλις ορίσαμε είναι το αμέσως προηγούμενο στάδιο πριν την εφαρμογή της αντίστροφης συνάρτησης f^{-1}, όπου f είναι η συνάτρηση κωδικοποίησης που είχαμε ορίσει στην παράγραφο 1.2 στη σελίδα 8.

Σχηματικά θα μπορούσαμε το όλο εγχείρημα "Κωδικοποίηση-Αποστολή-Λήψη-Αποκωδικοποίηση " να το παραστήσουμε ως εξής:



Παρατηρήσεις 1.3.2. 1. Όπως βλέπουμε η επιλογή και εφαρμογή της συνάρτησης φ αποτελούν πολύ σημαντικά βήματα στην όλη διαδικασία. Για το λόγο αυτό έχει επικρατήσει, αντί για κανόνα αποφασισιμότητας, να ονομάζουμε τη συνάρτηση φ **συνάρτηση αποκωδικοποίησης** και ως αποκωδικοποίηση να αναφέρεται η διαδικασία εφαρμογής της φ.

2. Λογικό θα ήταν η συνάρτηση f^{-1} να ονομάζεται συνάρτηση αποκωδικοποίησης, ως αντίστροφη της συνάρτησης κωδικοποίησης f και ως αποκωδικοποίηση η εφαρμογή της f^{-1}, όπως άλλωστε αναφέρεται στην παράγραφο 1.2. Μετά όμως από την προηγούμενη παρατήρηση δεν υπάρχει κίνδυνος σύγχυσης και θα χρησιμοποιούμε τον όρο αποκωδικοποίηση σε ότι έχει σχέση με τη συνάρτηση φ.

3. Στην περίπτωση, όπου $\varphi(\mathbf{x}) \in \mathcal{C}$ η διαδικασία συνεχίζεται. Αν $\varphi(\mathbf{x}) = ?$, οπότε αποφαινόμεθα ότι πρόκειται για λάθος, η διαδικασία σταματά και ο δέκτης είτε αγνοεί τη ληφθείσα λέξη, είτε (το λογικότερο, αν είναι δυνατον) ζητά την επανάληψη της αποστολής της *αμφισβητούμενης/ύποπτης* λέξης.

Έστω ότι έχει σταλεί μια λέξη $\mathbf{c} \in \mathcal{C}$ και έχει ληφθεί η λέξη $\mathbf{x} \in \mathbb{A}^n$. Η αποκωδικοποίηση είναι *σωστή* αν $\varphi(\mathbf{x}) = c$.

Υπάρχουν πολλοί τρόποι προσδιορισμού της συνάρτησης αποκωδικοποίησης, εδώ εμείς θα παρουσιάσουμε τους δύο πλέον γνωστούς τρόπους. (Στην πραγματικότητα, όπως θα δούμε, πρόκειται για δύο όψεις του *ιδίου νομίσματος*).

1.3.1 Η αρχή της αποκωδικοποίησης μέγιστης πιθανότητας

Μια *καλή* συνάρτηση αποκωδικοποίησης είναι μια συνάρτηση φ, η οποία μεγιστοποιεί την πιθανότητα σωστής αποκωδικοποιήσης. Δηλαδή (δεδομένου ότι ελήφθει η λέξη $\mathbf{x}$) η πιθανότητα να εστάλει η λέξη $\varphi(\mathbf{x})$ να είναι όσον το δυνατόν μεγαλύτερη.

Έστω φ μια συνάρτηση αποκωδικοποίησης. Υποθέτουμε ότι εστάλει η λέξη $\mathbf{c} \in \mathcal{C}$, δεδομένου ότι ελήφθει η λέξη $\mathbf{x}$, για μια σωστή αποκωδικοποίηση πρέπει να εχουμε $\varphi(\mathbf{x}) = \mathbf{c}$. Επομένως η (δεσμευμένη) πιθανότητα
$p(\mathbf{c} \mid \mathbf{c}) = p(\,\textit{έχουμε σωστή αποκωδικοποίηση} \mid \textit{δεδομένου ότι εστάλει η}\ \mathbf{c}\,) =$
$p(\,\varphi(\mathbf{x}) = \mathbf{c} \mid \textit{δεδομένου ότι εστάλει η}\ \mathbf{c}\,)$ είναι ίση με το άθροισμα όλων των πιθανοτήτων $p(\,\textit{ελήφθει η λέξη}\ \mathbf{x} \mid \textit{εστάλει η λέξη}\ \mathbf{c}\,)$, όπου το $\mathbf{x}$ διατρέχει όλες τις λέξεις στο $\mathbb{A}^n$ που ικανοποιούν τη σχέση $\varphi(\mathbf{x}) = c$. Δηλαδή $p(\mathbf{c} \mid \mathbf{c}) = \sum_{x \in \varphi^{-1}(\mathbf{c})} p(\,\textit{ελήφθει η λέξη}\ \mathbf{x} \mid \textit{εστάλει η λέξη}\ \mathbf{c}\,)$.

Έστω ότι ο κώδικας $\mathcal{C}$ αποτελείται από τις (κωδικο)λέξεις $\mathbf{c}_i,\ i = 1, \ldots, M$. Κατά την αποκωδικοποίηση μηνυμάτων σημασία έχουν οι **πιθανότητες αποστολής** $p(\mathbf{c}_i) =$ η πιθανότητα να έχει σταλεί η λέξη $\mathbf{c}_i$.

Παρατήρηση. Οι πιθανότητες αποστολής **δεν** εξαρτώνται από τον δίαυλο επικοινωνίας. Επομένως δεν πρέπει να συγχέονται με τις πιθανότητες μετάδοσης, οι οποίες καθορίζουν τον δίαυλο επικοινωνίας. Συνήθως εξαρτώνται από το είδος των μηνυμάτων που αποστέλλονται και είναι μεγάλο πρόβλημα για τον παραλήπτη να καθορίσει αυτές τις πιθανότητες. Μια ακραία περίπτωση, η οποία όμως απλοποιεί την κατάσταση, είναι η εξής: Κάνουμε την παραδοχή ότι για όλες τις λέξεις του κώδικα οι πιθανότητες αποστολής είναι ίσες, δηλαδή $p(\mathbf{c}_i) = 1/M$, για όλες τις λέξεις $\mathbf{c}_i,\ i = 1, 2, \ldots, M$ του κώδικα.

Από το Θεώρημα ολικής πιθανότητας προφανώς έχουμε
$p(\textit{σωστής αποκωδικοποίησης}) = \sum_{\mathbf{c} \in \mathcal{C}} p(\mathbf{c} \mid \mathbf{c}) \cdot p(\mathbf{c})$.
Οπότε από τα προηγούμενα έχουμε
$p(\textit{σωστής αποκωδικοποίησης}) =$
$= \sum_{\mathbf{c} \in \mathcal{C}} \sum_{x \in \varphi^{-1}(\mathbf{c})} p(\,\textit{ελήφθει η λέξη}\,\mathbf{x} \mid \textit{εστάλει η λέξη}\ \mathbf{c}\,) \cdot p(\mathbf{c})$.

Επομένως αν θέλουμε να μεγιστοποιήσουμε την πιθανότητα σωστής αποκωδικοποίησης θα πρέπει να βρούμε μια συνάρτηση αποκωδικοποίησης φ τέτοια ώστε $p(\,\textit{ελήφθει η λέξη}\ \mathbf{x} \mid \textit{εστάλει η λέξη}\ \varphi(\mathbf{x})\,) = \max\{\, p(\,\textit{ελήφθει η λέξη}\ \mathbf{x} \mid \textit{εστάλει η λέξη}\ \mathbf{c}\,) \mid c \in \mathcal{C}\,\}$ για όλες τις λέξεις $\mathbf{x}$ που είναι δυνατόν να ληφθούν (δηλαδή για όλα τα $\mathbf{x} \in \mathbb{A}^n$). Μια τέτοια συνάρτηση αποκωδικοποίησης θα λέγεται συνάρτηση **αποκωδικοποίησης μέγιστης πιθανότητας** και η αποκωδικοποίηση με τη βοήθεια μιας τέτοιας συνάρτησης θα λέγεται αποκωδικοποίηση ως προς την **αρχή της μέγιστης πιθανότητας** .

Στην σχέση της πιθανότητας σωστής αποκωδικοποίησης εμφανίζονται οι πιθανότητες μετάδοσης, καθότι, όπως γνωρίζουμε, σε έναν (αμνήμονα) δίαυλο ισχύει η σχέση $p(\ \epsilon\lambda\acute{\eta}\varphi\theta\epsilon\iota\ \eta\ \lambda\acute{\epsilon}\xi\eta\ \mathbf{x}\ \mid\ \ \epsilon\sigma\tau\acute{\alpha}\lambda\epsilon\iota\ \eta\ \lambda\acute{\epsilon}\xi\eta\ \mathbf{c}\ ) = \prod_{i=1}^{n} p(\epsilon\lambda\acute{\eta}\varphi\theta\epsilon\iota\ o\ x_i\ \mid\ \epsilon\sigma\tau\acute{\alpha}\lambda\epsilon\iota\ o\ c_i)$. Οπότε μπορούμε να αντικαταστήσουμε στην παραπάνω σχέση της πιθανότητας σωστής αποκωδικοποίησης.

Η σχέση που τελικά προκύπτει για τον υπολογισμό της πιθανότητας σωστής αποκωδικοποίησης είναι πολύ δύσχρηστη και δεν μπορεί να εφαρμοσθεί με ευχέρεια, δεδομένου ότι επιπλέον έχουμε και το πρόβλημα υπολογισμού των πιθανοτήτων αποστολής.

Θα μπορούσαμε να υπολογίσουμε την πιθανότητα σωστής αποκωδικοποίησης στηριζόμενοι όχι στις πιθανότητες μετάδοσης ενός διαύλου, αλλά δυϊκά στις πιθανότητες λήψης ενός διαύλου.

Ορισμός 1.3.3. *Σε ένα δίαυλο επικοινωνίας με αλφάβητο* $\mathbb{A} = \{ a_1, a_2, \ldots, a_r \}$ *οι (δεσμευμένες) πιθανότητες* $q_{ij} = p(\epsilon\sigma\tau\acute{\alpha}\lambda\epsilon\iota\ o\ \chi\alpha\rho\alpha\kappa\tau\acute{\eta}\rho\alpha\varsigma\ a_i\ \mid \epsilon\lambda\acute{\eta}\varphi\theta\epsilon\iota\ o\ \chi\alpha\rho\alpha\kappa\tau\acute{\eta}\rho\alpha\varsigma\ a_j)$ *ονομάζονται* **πιθανότητες λήψης**.

Δεν πρέπει να γίνεται σύγχυση μεταξύ των πιθανοτήτων μετάδοσης και των πιθανοτήτων λήψης. Στις μεν υποτίθεται ότι εστάλει μια λέξη, έστω $\mathbf{c} \in \mathcal{C}$ και ελήφθει μια λέξη $\mathbf{x} \in \mathbb{A}^n$. Στις δε υποτίθεται ότι ελήφθει μια λέξη $\mathbf{x} \in \mathbb{A}^n$ ενώ εστάλει η λέξη $\mathbf{c} \in \mathcal{C}$.

Προφανώς σε ένα αμνήμονα δίαυλο για τις πιθανότητες λήψης ισχύει ανάλογη σχέση με τη σχέση που ισχύει για τις πιθανότητες μετάδοσης.

Έστω η (κωδικο)λέξη $\mathbf{c} = c_1\, c_2 \cdots c_n$ και η λέξη $\mathbf{x} = x_1\, x_2 \cdots x_n$. Τότε η πιθανότητα $p(\ \epsilon\sigma\tau\acute{\alpha}\lambda\epsilon\iota\ \eta\ \lambda\acute{\epsilon}\xi\eta\ \mathbf{c}\ \mid\ \ \epsilon\lambda\acute{\eta}\varphi\theta\epsilon\iota\ \eta\ \lambda\acute{\epsilon}\xi\eta\ \mathbf{x}\ )$ είναι ίση με το γινόμενο των πιθανοτήτων λήψης $p(\epsilon\sigma\tau\acute{\alpha}\lambda\epsilon\iota\ o\ \chi\alpha\rho\alpha\kappa\tau\acute{\eta}\rho\alpha\varsigma\ c_i\ \mid\ \epsilon\lambda\acute{\eta}\varphi\theta\epsilon\iota\ o\ \chi\alpha\rho\alpha\kappa\tau\acute{\eta}\rho\alpha\varsigma\ x_i)$. Δηλαδή $p(\epsilon\sigma\tau\acute{\alpha}\lambda\epsilon\iota\ \eta\ \lambda\acute{\epsilon}\xi\eta\ \mathbf{c}\ \mid\ \ \epsilon\lambda\acute{\eta}\varphi\theta\epsilon\iota\ \eta\ \lambda\acute{\epsilon}\xi\eta\ \mathbf{x}\ ) =$
$\prod_{i=1}^{n} p(\epsilon\sigma\tau\acute{\alpha}\lambda\epsilon\iota\ o\ \chi\alpha\rho\alpha\kappa\tau\acute{\eta}\rho\alpha\varsigma\ c_i\ \mid\ \epsilon\lambda\acute{\eta}\varphi\theta\epsilon\iota\ o\ \chi\alpha\rho\alpha\kappa\tau\acute{\eta}\rho\alpha\varsigma\ x_i)$.

Επανερχόμενοι τώρα στον υπολογισμό της πιθανότητας σωστής αποκωδικοποίησης στηριζόμενοι στις πιθανότητες λήψης ενός διαύλου έχουμε.

$p(\sigma\omega\sigma\tau\acute{\eta}\varsigma\ \alpha\pi o\kappa\omega\delta\iota\kappa o\pi o\acute{\iota}\eta\sigma\eta\varsigma) =$
$\sum_{\mathbf{x}\in\mathbb{A}^n} p(\sigma\omega\sigma\tau\acute{\eta}\varsigma\ \alpha\pi o\kappa\omega\delta\iota\kappa o\pi o\acute{\iota}\eta\sigma\eta\varsigma\ \mid\ \epsilon\lambda\acute{\eta}\varphi\theta\epsilon\iota\ \eta\ \lambda\acute{\epsilon}\xi\eta\ \mathbf{x}) \cdot p(\epsilon\lambda\acute{\eta}\varphi\theta\epsilon\iota\ \eta\ \lambda\acute{\epsilon}\xi\eta\ \mathbf{x})$.

Όταν έχουμε μια συνάρτηση αποκωδικοποίησης φ μια ληφθείσα λέξη $\mathbf{x}$ αποκωδικοποιείται σωστά αν η λέξη που εστάλει είναι πράγματι η $\varphi(\mathbf{x})$. Οπότε $p(\sigma\omega\sigma\tau\acute{\eta}\varsigma\ \alpha\pi o\kappa\omega\delta\iota\kappa o\pi o\acute{\iota}\eta\sigma\eta\varsigma\ \mid\ \epsilon\lambda\acute{\eta}\varphi\theta\epsilon\iota\ \eta\ \lambda\acute{\epsilon}\xi\eta\ \mathbf{x}) = p(\epsilon\sigma\tau\acute{\alpha}\lambda\epsilon\iota\ \eta\ \lambda\acute{\epsilon}\xi\eta\ \varphi(\mathbf{x})\ \mid$ $\epsilon\lambda\acute{\eta}\varphi\theta\epsilon\iota\ \eta\ \lambda\acute{\epsilon}\xi\eta\ \mathbf{x}\ )$.

Αντικαθιστώντας στην προηγούμενη σχέση έχουμε
$p(\sigma\omega\sigma\tau\acute{\eta}\varsigma\ \alpha\pi o\kappa\omega\delta\iota\kappa o\pi o\acute{\iota}\eta\sigma\eta\varsigma) =$
$\sum_{\mathbf{x}\in\mathbb{A}^n} p(\ \epsilon\sigma\tau\acute{\alpha}\lambda\epsilon\iota\ \eta\ \lambda\acute{\epsilon}\xi\eta\ \varphi(\mathbf{x})\ \mid\ \ \epsilon\lambda\acute{\eta}\varphi\theta\epsilon\iota\ \eta\ \lambda\acute{\epsilon}\xi\eta\ \mathbf{x}\ ) \cdot p(\ \epsilon\lambda\acute{\eta}\varphi\theta\epsilon\iota\ \eta\ \lambda\acute{\epsilon}\xi\eta\ \mathbf{x})$.

Επομένως αν θέλουμε να μεγιστοποιήσουμε την πιθανότητα σωστής αποκωδικοποίησης θα πρέπει να βρούμε μια συνάρτηση αποκωδικοποίησης φ τέτοια ώστε

$p(\epsilon\sigma\tau\acute{\alpha}\lambda\epsilon\iota\ \eta\ \lambda\acute{\epsilon}\xi\eta\ \varphi(\mathbf{x})\ \mid\ \epsilon\lambda\acute{\eta}\varphi\theta\epsilon\iota\ \eta\ \lambda\acute{\epsilon}\xi\eta\ \mathbf{x}) =$
$= \max\{\, p(\epsilon\sigma\tau\acute{\alpha}\lambda\epsilon\iota\ \eta\ \lambda\acute{\epsilon}\xi\eta\ \mathbf{c}\ \mid\ \epsilon\lambda\acute{\eta}\varphi\theta\epsilon\iota\ \eta\ \lambda\acute{\epsilon}\xi\eta\ \mathbf{x})\ \mid\ c \in \mathcal{C}\,\}$ για όλες τις λέξεις $\mathbf{x}$ που είναι δυνατόν να ληφθούν (δηλαδή για όλα τα $\mathbf{x} \in \mathbb{A}^n$). Μια τέτοια συνάρτηση αποκωδικοποίησης θα λέγεται συνάρτηση **ιδανικού παρατηρητή** . Με άλλα λόγια μια συνάρτηση ιδανικού παρατηρητή είναι μια συνάρτηση αποκωδικοποίησης φ, τέτοια ώστε, δεδομένου ότι ελήφθει η λέξη $\mathbf{x}$, το πιθανότερο είναι να έχει σταλεί η (κωδικο)λέξη $\varphi(\mathbf{x})$.

Παρατήρηση 1.3.4. Εδώ δεν πρέπει να παραβλέψουμε το εξής ενδεχόμενο. Μπορεί να υπάρχουν δύο (κωδικο)λέξεις (ή και περισσότερες) $\mathbf{c}_i$ και $\mathbf{c}_j$ έτσι ώστε $p(\epsilon\sigma\tau\acute{\alpha}\lambda\epsilon\iota\ \eta\ \lambda\acute{\epsilon}\xi\eta\ \mathbf{c}_i\ \mid\ \epsilon\lambda\acute{\eta}\varphi\theta\epsilon\iota\ \eta\ \lambda\acute{\epsilon}\xi\eta\ \mathbf{x}) =$
$= p(\epsilon\sigma\tau\acute{\alpha}\lambda\epsilon\iota\ \eta\ \lambda\acute{\epsilon}\xi\eta\ \mathbf{c}_j\ \mid\ \epsilon\lambda\acute{\eta}\varphi\theta\epsilon\iota\ \eta\ \lambda\acute{\epsilon}\xi\eta\ \mathbf{x}) =$
$\max\{\, p(\epsilon\sigma\tau\acute{\alpha}\lambda\epsilon\iota\ \eta\ \lambda\acute{\epsilon}\xi\eta\ \mathbf{c}\ \mid\ \epsilon\lambda\acute{\eta}\varphi\theta\epsilon\iota\ \eta\ \lambda\acute{\epsilon}\xi\eta\ \mathbf{x})\ \mid\ c \in \mathcal{C}\,\}$. Στην περίπτωση αυτή υπάρχει πρόβλημα ως προς τον ορισμό της συνάρτησης φ. Θα θέσουμε $\varphi(\mathbf{x}) = \mathbf{c}_i$ ή $\varphi(\mathbf{x}) = \mathbf{c}_j$; Στην πράξη το θέμα αντιμετωπίζεται κατά περίπτωση. Τις περισσότερες φορές θέτουμε $\varphi(\mathbf{x}) = ?$, όπου εδώ το σύμβολο ? δεν δηλώνει ότι η λέξη $\mathbf{x}$ που λάβαμε είναι λανθασμένη, αλλά *αδυναμία* αποκωδικοποίησης. Υπάρχουν περιπτώσεις, όπου, αναλαμβάνοντας τον κίνδυνο λανθασμένης αποκωδικοποίησης, θέτουμε τυχαία η τιμή της συνάρτησης φ στη θέση $\mathbf{x}$ να είναι μια από τις (κωδικο)λέξεις που πληρούν τη σχέση $p(\epsilon\sigma\tau\acute{\alpha}\lambda\epsilon\iota\ \eta\ \lambda\acute{\epsilon}\xi\eta\ \mathbf{c}_i\ \mid\ \epsilon\lambda\acute{\eta}\varphi\theta\epsilon\iota\ \eta\ \lambda\acute{\epsilon}\xi\eta\ \mathbf{x}) =$
$\max\{\, p(\epsilon\sigma\tau\acute{\alpha}\lambda\epsilon\iota\ \eta\ \lambda\acute{\epsilon}\xi\eta\ \mathbf{c}\ \mid\ \epsilon\lambda\acute{\eta}\varphi\theta\epsilon\iota\ \eta\ \lambda\acute{\epsilon}\xi\eta\ \mathbf{x})\ \mid\ c \in \mathcal{C}\,\}$.

Όταν αναφερόμαστε για συναρτήσεις αποκωδικοποίησης μεγίστης πιθανότητας ή ιδανικού παρατηρητή, στην πραγματικότητα αναφερόμαστε στην ίδια συνάρτηση.

Πράγματι, από το Θεώρημα του Bayes έχουμε

$$p(\epsilon\sigma\tau\acute{\alpha}\lambda\epsilon\iota\ \eta\ \lambda\acute{\epsilon}\xi\eta\ \mathbf{c}\ \mid\ \epsilon\lambda\acute{\eta}\varphi\theta\epsilon\iota\ \eta\ \lambda\acute{\epsilon}\xi\eta\ \mathbf{x}) =$$

$$= \frac{p(\epsilon\lambda\acute{\eta}\varphi\theta\epsilon\iota\ \eta\ \lambda\acute{\epsilon}\xi\eta\ \mathbf{x}\ \mid\ \epsilon\sigma\tau\acute{\alpha}\lambda\epsilon\iota\ \eta\ \lambda\acute{\epsilon}\xi\eta\ \mathbf{c}\,)\cdot p(\mathbf{c})}{\sum_{i=1}^{M} p(\epsilon\lambda\acute{\eta}\varphi\theta\epsilon\iota\ \eta\ \lambda\acute{\epsilon}\xi\eta\ \mathbf{x}\ \mid\ \epsilon\sigma\tau\acute{\alpha}\lambda\epsilon\iota\ \eta\ \lambda\acute{\epsilon}\xi\eta\ \mathbf{c}_i\,)\cdot p(\mathbf{c}_i)}\ .$$

Στην προηγούμενη σχέση εμφανίζονται οι πιθανότητες αποστολής οι οποίες δεν εξαρτώνται από τον δίαυλο επικοινωνίας, αλλά από τη φύση του μηνύματος. Εδώ κάνουμε την παραδοχή ότι για όλες τις λέξεις του κώδικα οι πιθανότητες αποστολής είναι ίσες ($p(\mathbf{c}_i) = 1/M$, για όλες τις λέξεις $\mathbf{c}_i$, $i = 1, 2, \ldots, M$ του κώδικα). οπότε η προηγούμενη σχέση γίνεται

$$p(\epsilon\sigma\tau\acute{\alpha}\lambda\epsilon\iota\ \eta\ \lambda\acute{\epsilon}\xi\eta\ \mathbf{c}\ \mid\ \epsilon\lambda\acute{\eta}\varphi\theta\epsilon\iota\ \eta\ \lambda\acute{\epsilon}\xi\eta\ \mathbf{x}) =$$

$$= \frac{p(\epsilon\lambda\acute{\eta}\varphi\theta\epsilon\iota\ \eta\ \lambda\acute{\epsilon}\xi\eta\ \mathbf{x}\ \mid\ \epsilon\sigma\tau\acute{\alpha}\lambda\epsilon\iota\ \eta\ \lambda\acute{\epsilon}\xi\eta\ \mathbf{c}\,)}{\sum_{i=1}^{M} p(\epsilon\lambda\acute{\eta}\varphi\theta\epsilon\iota\ \eta\ \lambda\acute{\epsilon}\xi\eta\ \mathbf{x}\ \mid\ \epsilon\sigma\tau\acute{\alpha}\lambda\epsilon\iota\ \eta\ \lambda\acute{\epsilon}\xi\eta\ \mathbf{c}_i\,)}\ .$$

Επομένως, όπως είπαμε, για τη συνάρτηση ιδανικού παρατηρητή πρέπει να μεγιστοποιηθεί το πρώτο μέλος της παραπάνω σχέσεως. Τούτο όμως είναι ισοδύναμο με το να μεγιστοποιηθεί ο αριθμητής του δευτέρου μέλους (ο παρανομαστής είναι σταθερός καθότι το άθροισμα των πιθανοτήτων μετάδοσης εξαρτάται από το δίαυλο επικοινωνίας και δεν μεταβάλεται). Ο αριθμητής όμως δεν είναι τίποτε άλλο απο την πιθανότητα μετάδοσης, οπότε η συνάρτηση ιδανικού παρατηρητή είναι η συνάρτηση μέγιστης πιθανότητας.

Συνεπώς έχουμε αποδείξει το εξής σημαντικό θεώρημα.

Θεώρημα 1.3.5. *Με την υπόθεση ότι οι πιθανότητες αποστολής είναι ίσες για όλες τις λέξεις του κώδικα, η συνάρτηση ιδανικού παρατηρητή, όπως και η συνάρτηση μεγίστης πιθανότητας, εξασφαλίζει αποκωδικοποίηση μεγίστης πιθανότητας.*

Παράδειγμα 1.3.6. Έστω ότι έχουμε τον δυαδικό κώδικα $\mathcal{C} = \{\,000, 111\,\}$ και έναν συμμετρικό δίαυλο με πιθανότητα μετάδοσης λάθους χαρακτήρα ίση με 0.01, δηλαδή $p(\textit{ελήφθει ο χαρακτήρας } 1 \mid \textit{εστάλει ο χαρακτήρας } 0) =$
$= p(\textit{ελήφθει ο χαρακτήρας } 0 \mid \textit{εστάλει ο χαρακτήρας } 1) = 0.01,$
οπότε η πιθανότητα μετάδοσης σωστού χαρακτήρα είναι ίση με 0.99, δηλαδή
$p(\textit{ελήφθει ο χαρακτήρας } 0 \mid \textit{εστάλει ο χαρακτήρας } 0) =$
$= p(\textit{ελήφθει ο χαρακτήρας } 1 \mid \textit{εστάλει ο χαρακτήρας } 1) = 0.99.$ Υποθέτουμε ότι ο δέκτης λαμβάνει τη λέξη $\mathbf{x} = 100$ και θέλουμε να υπολογίσουμε την τιμή της συνάρτησης αποκωδικοποίησης μέγιστης πιθανότητας για τη λέξη $\mathbf{x} = 100$. Σύμφωνα με τα προηγούμενα η $\varphi(\mathbf{x})$ πρέπει να πληροί τη σχέση $p(\,\textit{ελήφθει η λέξη } \mathbf{x} \mid \textit{εστάλει η λέξη } \varphi(\mathbf{x})\,) = \max\{\,p(\textit{ελήφθει η λέξη } \mathbf{x} \mid \textit{εστάλει η λέξη } 000\,),\ p(\,\textit{ελήφθει η λέξη } \mathbf{x} \mid \textit{εστάλει η λέξη } 111\,)\,\}$. Αλλά από τη σχέση (1.2.1) έχουμε $p(\,\textit{ελήφθει η λέξη } 100 \mid \textit{εστάλει η λέξη } 000\,) = (0.01)(0.99)^2 = 0.009801$ και $p(\,\textit{ελήφθει η λέξη } 100 \mid \textit{εστάλει η λέξη } 000\,) = (0.99)(0.01)^2 = 0.00099$. Επειδή η πρώτη πιθανότητα είναι μεγαλύτερη από τη δεύτερη, συμφωνα με την αρχή της αποκωδικοποίσης ως προς την μέγιστη πιθανότητα πρέπει να έχουμε $\varphi(\mathbf{x}) = 000$, δηλαδή η λέξη $\mathbf{x} = 100$ αποκωδικοποιείται ως η λέξη 000.

1.3.2 Η Αρχή της αποκωδικοποίησης ως προς την πλησιέστερη λέξη

Ας ξεκινήσουμε την παράγραφο με το τελευταίο παράδειγμα. Έστω ότι έχουμε τον κώδικα $\mathcal{C} = \{\,000, 111\,\}$ και ο δέκτης λαμβάνει τη λέξη 100, η οποία δεν ανήκει στον κώδικα. Λογικό είναι να υποτεθεί, ότι το πιθανότερο είναι να εστάλει η λέξη 000, η οποία είναι πλησιέστερη στην λέξη που ελήφθει. Οπότε αποκωδικοποιείται σαν 000.

Έστω ότι έχει σταλεί μια λέξη $\mathbf{c} \in \mathcal{C}$ και έχει ληφθεί η λέξη $\mathbf{x} \in \mathbb{A}^n$. Η αποκωδικοποίηση είναι *σωστή* αν $\varphi(\mathbf{x}) = c$.

Γενικά μια συνάρτηση αποκωδικοποίησης **ως προς την πλησιέστερη λέξη** την ορίζουμε ως εξής. Έστω ότι έχει σταλεί μια λέξη $\mathbf{c} \in \mathcal{C}$ και έχει ληφθεί η λέξη $\mathbf{x} \in \mathbb{A}^n$. Αν η $\mathbf{x}$ ανήκει στον κώδικα, τότε ορίζουμε $\varphi(\mathbf{x}) = \mathbf{x}$, δηλαδή κατά την αποκωδικοποίηση δεχόμαστε ότι εστάλει η λέξη $\mathbf{x}$. Αν η $\mathbf{x}$ δεν ανήκει στο κώδικα, τότε υπολογίζουμε την απόσταση της $\mathbf{x}$ από όλες τις άλλες λέξεις του κώδικα. Τότε υπάρχει μια λέξη $\mathbf{d}$ του κώδικα με την μικρότερη απόσταση από την $\mathbf{x}$. Αν η λέξη $\mathbf{d}$ είναι η μοναδική με την ιδιότητα αυτή, τότε ορίζουμε $\varphi(\mathbf{x}) = \mathbf{d}$ και κατά την αποκωδικοποίηση δεχόμαστε την $\mathbf{d}$. Αν υπάρχουν περισσότερες λέξεις οι οποίες απέχουν την ίδια ελάχιστη απόσταση από τη λέξη $\mathbf{x}$, τότε προς αποφυγή *σύγχυσης* δηλώνουμε *αδυναμία* αποκωδικοποίησης.

Η αποκωδικοποίηση με τη βοήθεια μιας τέτοιας συνάρτησης θα λέγεται αποκωδικοποίηση ως προς την **αρχή της πλησιέστερης λέξης** .

Παρατηρήσεις 1.3.7. 1. Η Αρχή της αποκωδικοποίησης ως προς την πλησιέστερη λέξη είναι ένας *φυσιολογικός* τρόπος αποκωδικοποίησης, τουλάχιστον στην αρχή. Στην πράξη όμως παρουσιάζει δυσκολίες σε κώδικες με μεγάλο μήκος, καθώς είναι αρκετά χρονοβόρο κάθε φορά να ελέγχουμε την απόσταση μιας λέξης που λαμβάνουμε από όλες τις λέξεις του κώδικα για να την αντικαταστήσουμε με την πλησιέστερη προς αυτή λέξη του κώδικα. Ένα καίριο μέλημα στο σχεδιασμό ενός κώδικα είναι η δυνατότητα ο έλεγχος αυτός να γίνεται γρήγορα και αποτελεσματικά. (Βλέπε Παράγραφο 2.3.4).

2. Η Αρχή της αποκωδικοποίησης ως προς την πλησιέστερη λέξη δεν αποκλείει το ενδεχόμενο να έχει σταλεί μια λέξη $\mathbf{c}$ κατά την μετάδοση να έχει παρισφύσει λάθος και να λάβουμε μια λέξη $\mathbf{x}$, η οποία να ανήκει στον κώδικα, οπότε η λέξη $\mathbf{c}$ αποκωδικοποιείται (κακώς βέβαια) σαν λέξη $\mathbf{x}$.

3. Έχουμε δεί ότι κατά την αποκωδικοποίηση είτε με την αρχή της μέγιστης πιθανότητας, είτε με την αρχή ως προς την πλησιέστερη λέξη ενδέχεται να έχουμε αδυναμία αποκωδικοποίησης. Στην περίπτωση αυτή έχει επικρατήσει η όλη διαδικασία να ονομάζεται **μη πλήρης αποκωδικοποίηση** . Ορισμένες φορές όμως, όπως έχουμε προείπει, αναλαμβάνοντας τον κίνδυνο λανθασμένης αποκωδικοποίησης, θέτουμε τυχαία η τιμή της συνάρτησης αποκωδικοποίησης φ στη θέση $\mathbf{x}$ της ληφθείσας λέξης να είναι μια από τις (κωδικο)λέξεις που πληρούν τη σχέση μεγίστης πιθανότητας, ή να είναι από τις πλησιέστερες στη λέξη $\mathbf{x}$. Στην περίπτωση αυτή η όλη διαδικασία ονομάζεται **πλήρης αποκωδικοποίηση** . Το τι είναι προτιμητέο εξαρτάται από την περίπτωση και δεν θα ασχοληθούμε εδώ.

Παραδείγματα 1.3.8. 1. Έστω ότι έχουμε τον κώδικα $\mathcal{C} = \{\, 0000,\, 0011,\, 1000,\, 1100 \,\}$ και έχει σταλεί η (κωδικο)λέξη $\mathbf{a} = 0011$. Τότε λαμβάνοντας τη λέξη $\mathbf{x} = 0111$, παρατηρούμε ότι η μικρότερη απόσταση της $\mathbf{x}$ από τα στοιχεία του κώδικα είναι (μόνο) από την (κωδικο)λέξη $\mathbf{a}$ (αυτή που εστάλει), οπότε ορθώς αποκωδικοποιούμε την $\mathbf{x}$ σαν $\mathbf{a}$. Αν όμως λάβουμε την λέξη $\mathbf{y} = 1001$, τότε βλέπουμε ότι αυτή η λέξη ισαπέχει από τις (κωδικο)λέξεις 0000 και 0011, οπότε δεν μπορούμε να την αποδικωποιήσουμε. Τέλος δεν αποκλείεται να λάβουμε τη λέξη $\mathbf{z} = 0000$, δηλαδή να έχει επέλθει αλλοίωση σε δύο χαρακτήρες και να την δεχθούμε, λανθασμένα, ως τη λέξη που εστάλει, αφού και αυτή ανήκει στον κώδικα.

2. Ας επανέλθουμε στο Παράδειγμα της σελίδας 12, όπου ζητείται η ασφαλής καθοδήγηση ενός πλοίου μέσω κωδικοποιημένου μηνύματος.

   Αντί του κώδικα $\mathcal{D} = \{\, 000,\, 011,\, 101,\, 110 \,\}$ χρησιμοποιούμε τον κώδικα $\mathcal{E} = \{\, 00000,\, 01101,\, 10110,\, 11011 \,\}$ και συνάρτηση κωδικοποίησης $h : S \longrightarrow \mathcal{E}$ με $h(\mathbf{A}) = 00000$, $h(\mathbf{\Delta}) = 01101$, $h(\mathbf{B}) = 10110$, $h(\mathbf{N}) = 11011$. Παρατηρούμε ότι ο κώδικας $\mathcal{E}$ προέρχεται από τον προηγούμενο κώδικα επισυνάπτοντας δύο επιπλέον ψηφία με τέτοιο τρόπο ώστε δύο κωδικολέξεις να απέχουν μεταξύ τους απόσταση τουλάχιστον ίση με τρία. Υποθέτουμε ότι εστάλει η (κωδικο)λέξη $\mathbf{a} = 01101$ και ελήφθει η λέξη $\mathbf{x} = 01111$. Η ληφθείσα λέξη δεν ανήκει στον κώδικα, αλλά η μικρότερη απόστασή της από τα στοιχεία του κώδικα είναι (μόνο) από την (κωδικο)λέξη $\mathbf{a} = 01101$ που εστάλει. Οπότε σύμφωνα με την αρχή ως προς την πλησιέστερη λέξη μπορεί ορθώς να αποκωδικοποιηθεί ως η $\mathbf{a} = 01101$. Δηλαδή με τη βοήθεια του κώδικα το λάθος όχι μόνο "ανιχνεύθηκε", αλλά "διορθώθηκε". Αν όμως κατά την αποστολή υπησήλθαν λάθη σε περισσότερες από μία θέσεις και ελήφθει η λέξη $\mathbf{y} = 11111$, τότε ανιχνεύται λάθος, αφού η $\mathbf{y} = 11111$ δεν ανήκει στον κώδικα, αλλά αν επιχειρηθεί να αποκωδικοποιηθεί σύμφωνα με την αρχή ως προς την πλησιέστερη λέξη, τότε αποκωδικοποιείται λανθασμένα ως η $\mathbf{b} = 11011$.

Τα παραπάνω προβλήματα που παρουσιάζονται κατά την αποκωδικοποίηση με αυτό τον τρόπο θα μπορούσαν να εξαλειφθούν, αν μη τι άλλο να περιοριστούν, αν ο κώδικας είχε επιλεγεί ώστε οι λέξεις του να ήταν *αραιά* κατενεμημένες. Για να γίνουμε πιο συγκεκριμένοι χρειαζόμαστε μερικούς ορισμούς:

Ορισμός 1.3.9. *Έστω $\mathcal{C}$ ένας κώδικας (με τουλάχιστον δύο λέξεις). Η* **ελάχιστη απόσταση** *$d(\mathcal{C})$ του $\mathcal{C}$ είναι η μικρότερη απόσταση μεταξύ δύο διακεκριμένων λέξεων. Δηλαδή $d(\mathcal{C}) = \min\{\, d(\mathbf{c}, \mathbf{d}) \mid \mathbf{c}, \mathbf{d} \in \mathcal{C}, \mathbf{c} \neq \mathbf{d} \,\}$.*

Επομένως εκτός από το αλφάβητο, το μήκος n και το μέγεθος του $M = |\, \mathcal{C} \,|$

ενός κώδικα $\mathcal{C}$ έχουμε μια επιπλέον παράμετρο, την ελάχιστη απόσταση $d = d(\mathcal{C})$ του κώδικα, και για συντομία θα αναφέρεται ως ένας (n, M, d) κώδικας.

Ορισμός 1.3.10. *Ένα διάνυσμα λάθους* $\mathbf{e} \in \mathbb{A}^n$ **ανιχνεύεται** *από έναν* **p**-*αδικό κώδικα* $\mathcal{C} \subseteq \mathbb{A}^n$ *αν η λέξη* $\mathbf{a}+\mathbf{e}$ *δεν ανήκει στο κώδικα* $\mathcal{C}$ *για κάθε (κωδικο)λέξη* $\mathbf{a} \in \mathcal{C}$. *Αν υπάρχει (τουλάχιστον ένα)* $\mathbf{a} \in \mathcal{C}$ *έτσι ώστε* $\mathbf{a}+\mathbf{e} \in \mathcal{C}$, *τότε το διάνυσμα* $\mathbf{e}$ *είναι* **μη ανιχνεύσιμο**.

Ένας κώδικας $\mathcal{C}$ **ανιχνεύει** λ *λάθη, όπου* λ *είναι ένας θετικός ακέραιος αριθμός, αν κάθε διάνυσμα λάθους* $\mathbf{e}$ *βάρους το πολύ* λ *ανιχνεύεται από τον κώδικα* $\mathcal{C}$. *Ένας κώδικας* $\mathcal{C}$ **ανιχνεύει ακριβώς** λ *λάθη, αν ανιχνεύει (διανύσματα) λάθους με βάρος το πολύ* λ, *αλλά δεν ανιχνεύει λάθη με βάρος* $\lambda+1$.

Τονίζουμε, σύμφωνα με τον προηγούμενο ορισμό, όταν λέμε ο κώδικας ανιχνεύει λ λάθη, εννοούμε ότι, αν κατά τη μετάδοση μιας λέξης έχουν επέλθει αλλοιώσεις το πολύ σε λ το πλήθος χαρακτήρες, τότε έχουμε απλώς την ένδειξη ότι η ληφθείσα λέξη δεν ανήκει στον κώδικα, **χωρίς** καμία άλλη πληροφορία για το διάνυσμα λάθους που υπεισήλθε.

Ας φαντασθούμε ότι έχουμε ένα μηχανισμό (π. χ. έναν υπολογιστή) που ελέγχει τις λέξεις που καταφθάνουν και ότι όταν εντοπίζεται μία λέξη που δεν ανήκει στο κώδικα, τότε ανάβει μια κόκκινη λυχνία. Αν ο κώδικας ανιχνεύει λ λάθη, τότε η λυχνία ανάβει (οπωσδήποτε), αν κατά τη μετάδοση μιας λέξης έχουν επέλθει αλλοιώσεις το πολύ σε λ το πλήθος χαρακτήρες. Ενδέχεται όμως η λυχνία να ανάβει (ή να μην ανάβει), όταν υπεισέρχονται διανύσματα λάθους με βάρος μεγαλύτερο του λ. Καθότι, όπως έχουμε παρατηρήσει, ενδέχεται η αποσταλείσα λέξη να έχει υποστεί τόσες πολλές αλλοιώσεις κατά τη μετάδοση έτσι ώστε να έχουμε λάβει μια άλλη λέξη του κώδικα.

Παράδειγμα 1.3.11. Ο κώδικας $\mathcal{C} = \{\,0000,\, 0011,\, 1000,\, 1100\,\}$ δεν ανιχνεύει κανένα λάθος (γιατί;). Ο κώδικας $\mathcal{C} = \{\,000000,\, 111000,\, 111111\,\}$ ανιχνεύει δύο λάθη (γιατί;), ενώ δεν ανιχνεύει όλα τα τρία λάθη π.χ. αν έχει σταλεί η λέξη 000000, ανιχνεύει τη λανθασμένη λέξη 010101, αλλά δεν ανιχνεύει τη λανθασμένη λέξη 111000. (Μάλιστα δε, σύμφωνα με την Αρχή της αποκωδικοποίησης ως προς την πλησιέστερη λέξη, την αποκωδικοποιεί λανθασμένα).

Ορισμός 1.3.12. *Ένα διάνυσμα λάθους* $\mathbf{e} \in \mathbb{A}^n$ **διορθώνεται** *από έναν* **p**-*αδικό κώδικα* $\mathcal{C} \subseteq \mathbb{A}^n$ *αν για κάθε σταλείσα λέξη* $\mathbf{a} \in \mathcal{C}$ *η ληφθείσα λέξη* $\mathbf{a}+\mathbf{e}$, *που δεν ανήκει στο κώδικα* $\mathcal{C}$, *αποκωδικοποιείται, σύμφωνα με την Αρχή της αποκωδικοποίησης ως προς την πλησιέστερη λέξη, ως η λέξη* $\mathbf{a} \in \mathcal{C}$.

Ένας κώδικας $\mathcal{C}$ **διορθώνει** λ *λάθη, όπου* λ *είναι ένας θετικός ακέραιος αριθμός, αν κάθε διάνυσμα λάθους* $\mathbf{e}$ *βάρους το πολύ* λ *διορθώνεται από τον κώδικα* $\mathcal{C}$. *Ένας κώδικας* $\mathcal{C}$ **διορθώνει ακριβώς** λ *λάθη, αν διορθώνει (διανύσματα) λάθους με βάρος το πολύ* λ, *αλλά δεν διορθώνει λάθη με βάρος* $\lambda+1$.

Τονίζουμε, σύμφωνα με τον προηγούμενο ορισμό, όταν λέμε ο κώδικας διορθώνει λ λάθη, εννοούμε ότι, αν κατά τη μετάδοση μιας λέξης έχουν επέλθει αλλοιώσεις το πολύ σε λ το πλήθος χαρακτήρες, τότε ο παραλήπτης είναι σίγουρος ότι κατά την αποκωδικοποίηση θα λάβει την λέξη που έχει σταλεί χωρίς καμία επιπλέον πληροφορία για το διάνυσμα λάθους. Αν όμως κατά τη μετάδοση μιας λέξης έχουν επέλθει αλλοιώσεις σε περισσότερους από λ το πλήθος χαρακτήρες, τότε ο παραλήπτης δεν είναι σίγουρος κατά την αποκωδικοποίηση ότι η λέξη που έλαβε είναι πράγματι η λέξη που έχει σταλεί.

Παρατηρήσεις 1.3.13.

1. Αν θέλουμε να εκφράσουμε τη διόρθωση λαθών με τη βοήθεια της συνάρτησης αποκωδικοποίησης φ, μπορούμε να πούμε ότι το διάνυσμα λάθους $\mathbf{e} \in \mathbb{A}^n$ διορθώνεται αν για κάθε σταλείσα λέξη $\mathbf{a} \in \mathcal{C}$ ισχύει $\varphi(\mathbf{a}+\mathbf{e}) = \mathbf{a}$.

2. Όταν λέμε ότι ένας κώδικας δεν διορθώνει λάθη βάρους $\lambda+1$, εννούμε ότι υπάρχει τουλάχιστον ένα $\mathbf{e} \in \mathbb{A}^n$ με βάρος $\lambda+1$ και, τουλάχιστον, μία (κωδικο)λέξη $\mathbf{a} \in \mathcal{C}$ έτσι ώστε, αν έχει σταλεί η (κωδικο)λέξη $\mathbf{a}$ και έχει ληφθεί η λέξη $\mathbf{x} = \mathbf{a}+\mathbf{e}$, να έχουμε $\varphi(\mathbf{a}+\mathbf{e}) \neq \mathbf{a}$.

3. Όταν ένας κώδικας διορθώνει λ λάθη, τότε αμέσως παρατηρούμε ότι ισχύει $d(\mathcal{C}) \geq \lambda+1$. (γιατί ;) Συγκεκριμένα ισχύει κάτι πολύ ισχυρότερο (Βλέπε Θεώρημα 1.3.16).

Μπορούμε να αναδιατυπώσουμε τον ορισμό πότε ένας κώδικας ανιχνεύει ένα λάθος χρησιμοποιώντας την έννοια της ελάχιστης απόστασης ενός κώδικα.

Θεώρημα 1.3.14. *Ένας κώδικας $\mathcal{C}$ ανιχνεύει λ λάθη αν και μόνο αν $d(\mathcal{C}) \geq \lambda+1$.*

Απόδειξη. Όπως προείπαμε, η απόδειξη αποτελεί αναδιατύπωση του ορισμού και αφίνεται ως άσκηση.

□

Πρόταση 1.3.15. *Ένας κώδικας $\mathcal{C}$ ανιχνεύει ακριβώς λ λάθη αν και μόνο αν $d(\mathcal{C}) = \lambda+1$.*

Απόδειξη. Άσκηση. □

Όπως "διαισθανόμαστε", ένας κώδικας για να διορθώνει λάθη, και όχι απλώς να ανιχνεύει, πρέπει να είναι αρκετά "αραιός". Συγκεκριμένα ισχύει το εξής θεώρημα.

Θεώρημα 1.3.16. *Ένας κώδικας $\mathcal{C}$ διορθώνει λ λάθη αν και μόνο αν $d(\mathcal{C}) \geq 2\lambda+1$.*

Απόδειξη. Υποθέτουμε ότι $d(\mathcal{C}) \geq 2\lambda + 1$. Έστω ότι εστάλει η λέξη $\mathbf{a} \in \mathcal{C}$ και ελήφθει η λέξη $\mathbf{b} = \mathbf{a}+\mathbf{e}$, που δεν ανήκει στο κώδικα $\mathcal{C}$, όπου $\mathbf{e}$ είναι το διάνυσμα λάθους που υπεισήλθε και επέφερε αλλοιώσεις σε λ (το πολύ) χαρακτήρες. Τότε προφανώς $1 \leq d(\mathbf{a}, \mathbf{b}) \leq \lambda$. Η λέξη $\mathbf{b}$ είναι πλησιέστερα στη λέξη $\mathbf{a}$ από κάθε άλλη λέξη του κώδικα. Πράγματι, αν υπήρχε μια άλλη λέξη $\mathbf{c} \in \mathcal{C}$ με $d(\mathbf{b}, \mathbf{c}) \leq d(\mathbf{b}, \mathbf{a})$, τότε από την τριγωνική ιδιότητα έχουμε

$$d(\mathbf{a}, \mathbf{c}) \leq d(\mathbf{a}, \mathbf{b}) + d(\mathbf{b}, \mathbf{c}) \leq \lambda + \lambda < d(\mathcal{C}).$$

Άτοπο. Επομένως αφού η λέξη $\mathbf{b}$ που ελήφθει είναι πλησιέστερα προς τη λέξη $\mathbf{a}$ που εστάλει, αποκωδικοποιείται (ορθώς) ως η λέξη $\mathbf{a}$ και ο κώδικας διωρθώνει λ λάθη.

Αντίστροφα, υποθέτουμε ότι ο κώδικας $\mathcal{C}$ διορθώνει λ λάθη. Από προηγούμενη παρατήρηση έχουμε ότι $d(\mathcal{C}) \geq \lambda + 1$. Υποθέτουμε ότι $d(\mathcal{C}) \leq 2\lambda$. Έστω δύο λέξεις $\mathbf{a}, \mathbf{b} \in \mathcal{C}$, με $d(\mathbf{a}, \mathbf{b}) = d(\mathcal{C})$. Θα αποδείξουμε ότι ενδέχεται να σταλεί η λέξη $\mathbf{a}$, να υπεισέλθουν λ λάθη ώστε να ληφθεί μια λέξη, έστω $\mathbf{c}$, η οποία είτε να ισαπέχει από τις λέξεις $\mathbf{a}$ και $\mathbf{b}$, είτε να είναι πλησιέστερα προς τη λέξη $\mathbf{b}$. Οπότε, κατά την αποκωδικωποίηση, θα έχουμε αδυναμία αποκωδικοποίησης ή λάθος αποκωδικοποίηση ως η λέξη $\mathbf{b}$ αντί (του ορθού) ως η λέξη $\mathbf{a}$. Αυτό θα είναι άτοπο, καθότι υποθέσαμε ότι ο κώδικας διορθώνει λ λάθη.

Έστω ότι οι λέξεις $\mathbf{a} = (a_1, a_2, \ldots, a_n)$ και $\mathbf{b} = (b_1, b_2, \ldots, b_n)$ συμπίπτουν σε $n - d(\mathcal{C})$ το πλήθος θέσεις. Δηλαδή $a_{i_j} = b_{i_j}$ για
$j = 1, 2, \ldots, n - d(\mathcal{C})$. Υποθέτουμε ότι, αντί της λέξης $\mathbf{a}$ που εστάλει, ελήφθει η λέξη $\mathbf{c} = (c_1, c_2, \ldots, c_n)$, η οποία συμπίπτει στις ίδιες, $n - d(\mathcal{C})$ το πλήθος, θέσεις με τις λέξεις $\mathbf{a}$ και $\mathbf{b}$, δηλαδή $a_{i_j} = b_{i_j} = c_{i_j}$ για $j = 1, 2, \ldots, n-d(\mathcal{C})$. Για τις υπόλοιπες $d(\mathcal{C})$ το πλήθος θέσεις υποθέτουμε ότι η $\mathbf{c}$ συμπίπτει σε $d(\mathcal{C})-\lambda$ το πλήθος θέσεις με τη λέξη $\mathbf{a}$ και σε λ το πλήθος θέσεις με τη λέξη $\mathbf{b}$. Τότε η λέξη $\mathbf{c}$ διαφέρει από τη λέξη $\mathbf{a}$ σε λ το πλήθος θέσεις και από τη λέξη $\mathbf{b}$ σε $d(\mathcal{C})-\lambda$ το πλήθος θέσεις. Άρα $d(\mathbf{b}, \mathbf{c}) = d(\mathcal{C}) - \lambda \leq d(\mathbf{a}, \mathbf{c}) = \lambda$. Επομένως κατά την αποκωδικοποίηση αποκλείεται η λέξη να αποκωδικοποιηθεί ως η λέξη $\mathbf{a}$. Άτοπο. (Στην καλλίτερη περίπτωση θα είχαμε $d(\mathbf{b}, \mathbf{c}) = d(\mathcal{C}) - \lambda = d(\mathbf{a}, \mathbf{c}) = \lambda$).

□

Πρόταση 1.3.17. *Ένας κώδικας $\mathcal{C}$ διορθώνει ακριβώς λ λάθη αν και μόνο αν $d(\mathcal{C}) = 2\lambda + 1$ ή $d(\mathcal{C}) = 2\lambda + 2$.*

Απόδειξη. Η απόδειξη είναι απλή, και αποτελεί μια καλή άσκηση στην κατανόηση της διαφοράς μεταξύ του· ένας κώδικας διορθώνει (μέχρι) λ λάθη και του· ένας κώδικας διορθώνει ακριβώς λ λάθη.

□

Παρατήρηση 1.3.18. Από το προηγούμενα συνάγουμε ότι στη διόρθωση λαθών είναι " προτιμιταίοι " κώδικες με περιττή ελάχιστη απόσταση. Πράγματι, έστω ένας κώδικας $\mathcal{C}$ με ελάχιστη απόσταση $d(\mathcal{C}) = 2k+2$. Ο μέγιστος αριθμός λαθών που μπορεί να διορθώσει ο κώδικας, σύμφωνα με το προηγούμενο θεώρημα, είναι ίσος με $\lambda = \left[\frac{2k+2-1}{2}\right] = \left[\frac{2k+1}{2}\right] = k$. Αν "πλουτίσουμε " [6] τον κώδικα επισυνάπτοντας επιπλέον (κωδικο)λέξεις έτσι ώστε η ελάχιστη απόσταση του νέου κώδικα να μικρύνει και να γίνει ίση με $2k+1$, τότε ο νέος κώδικας μπορεί να διορθώσει πάλι μέχρι $\lambda = \left[\frac{2k+1-1}{2}\right] = \left[\frac{2k}{2}\right] = k$.

Παράδειγμα 1.3.19. (Ο κώδικας ISBN)

Όλοι γνωρίζουμε ότι σε κάθε βιβλίο αντιστοιχεί ένας δεκαψήφιος αριθμός (ο οποίος συνήθως αναγράφεται στο οπισθόφυλλο του βιβλίου) είναι ο γνωστός αριθμός ISBN (International Standard Book Number). Ο αριθμός αποτελεί την *ταυτότητα* του βιβλίου και περικλείει πληροφορίες για το βιβλίο. Το πρώτο ψηφίο δηλώνει τη γλώσσα στην οποία είναι γραμμένο το βιβλίο, τα επόμενα τρία ψηφία δηλώνουν τον εκδοτικό οίκο, τα επόμενα πέντε ψηφία δίνονται από τον εκδότη και το τελευταίο ψηφίο υπολογίζεται από τα προηγούμενα ως εξής:

Υποθέτουμε ότι έχουμε τον αριθμό $a_1a_2\cdots a_9a_{10}$, τα ψηφία $a_i,\ i = 1, \ldots, 9$ λαμβάνουν τιμές από το σύνολο $\{0, 1, \ldots, 9\}$. Εφ' όσον έχουν επιλεγεί τα $a_i,\ i = 1, \ldots, 9$, για το τελευταίο ψηφίο απαιτούμε να ισχύει
$a_{10} \equiv \sum_{i=1}^{9} i \cdot a_i (\mathrm{mod})11$. Δηλαδή το a_{10} είναι το υπόλοιπο της διαίρεσης του αθροίσματος $\sum_{i=1}^{9} i \cdot a_i$ με το 11. Το υπόλοιπο αυτό ενδέχεται να λαμβάνει και την τιμή 10, επειδή το "ψηφίο " 10 έχει δύο χαρακτήρες, για διαχειριστικούς καθαρά λόγους, έχει συμφωνηθεί στην περίπτωση αυτή να γράφουμε τον χαρακτήρα X.

Για παράδειγμα οι αριθμοί 0 387 94704 3 και 0 201 02988 X ικανοποιούν τις παραπάνω απαιτήσεις, άρα θα μπορούσαν να είναι οι ISBN για κάποια βιβλία.

Έστω $\mathcal{C}$ το σύνολο που αποτελείται από όλους τους δεκαψήφιους "αριθμούς" που υπολογίζονται σύμφωνα με την παραπάνω διαδικασία. Το $\mathcal{C}$ είναι ο κώδικας ISBN.

Ο κώδικας αυτός με τον τρόπο που σχεδιάστηκε μπορεί να ανιχνεύει ένα λάθος. Πράγματι, υποθέτουμε ότι εστάλει η (κωδικο)λέξη $\mathbf{a} = a_1a_2\cdots a_9a_{10}$, αλλά ελήφθει η λέξη $\mathbf{x} = x_1x_2\cdots x_9x_{10}$, η οποία συμφωνεί σε όλους τους χαρακτήρες με την $\mathbf{a}$, εκτός από τον χαρακτήρα a_r, όπου αντί αυτού έχουμε τον χαρακτήρα $x_r = a_r + e$ με $e \neq 0$. Από τον τρόπο ορισμού του κώδικα $\mathcal{C}$ έχουμε $\sum_{i=1}^{10} i \cdot a_i \equiv 0(\mathrm{mod})11$ (γιατί;). Αλλά για την λέξη $\mathbf{x}$ έχουμε

[6] Στην παράγραφο 1.4 θα αναφερθούμε διεξοδικότερα στο τί σημαίνει " προτιμιταίος " και τι "πλουσιώτερος " κώδικας.

$\sum_{i=1}^{10} i \cdot x_i = (\sum_{i=1}^{10} i \cdot a_i) + r \cdot e \neq 0(\text{mod})11$. Άρα ανιχνεύθηκε το λάθος.

Παρατηρήσεις. Στο προηγούμενο παράδειγμα θα πρέπει να παρατηρήσουμε τα εξής:

1. Στην τελευταία σχέση ισχυριζόμαστε ότι $r \cdot e \neq 0(\text{mod})11$. Αυτό πράγματι ισχύει διότι τα r και e είναι θετικοί ακέραιοι μικρότεροι ή ισοι του 10 διάφοροι του μηδενός, επομένως, επειδή ο πολλαπλασιασμός γίνεται στο σώμα $\mathbb{Z}_{11}$, το γινόμενό τους δεν είναι ίσο με το $0(\text{mod})11$.

2. Το συμπέρασμα ότι ο κώδικας ανιχνεύει ένα λάθος συνάδει με το Θεώρημα 1.3.14. Μάλιστα ανιχνεύει ακριβώς ένα λάθος καθότι η ελάχιστη απόστασή του είναι ίση με δύο, αφού για παράδειγμα τα 0 387 94704 3 και 2 387 94704 5 είναι στοιχεία του και διαφέρουν σε δύο μόνο χαρακτήρες.

3. Ο κώδικας ISBN δεν διορθώνει κανένα λάθος, παρ' όλα αυτά είναι *ικανοποιητικός* για τον σκοπό που έχει σχεδιασθεί. Διότι επιπλέον έχει τη δυνατότητα να ανιχνεύει τον "αναγραμματισμό" δύο χαρακτήρων σε μια (κωδικο)λέξη.

   Πράγματι, υποθέτουμε ότι εστάλει η (κωδικο)λέξη $\mathbf{a} = a_1a_2\cdots a_9a_{10}$, αλλά ελήφθει η λέξη $\mathbf{x} = x_1x_2\cdots x_9x_{10}$, της οποίας όλοι οι χαρακτήρες συμφωνούν με τους χαρακτήρες της $\mathbf{a}$, εκτός από τις θέσεις r και j, όπου οι χαρακτήρες έχουν αλλάξει θέση, δηλαδή $x_r = a_j$ και $x_j = a_r$. Τότε θα έχουμε $\sum_{i=1}^{10} i \cdot x_i = (\sum_{i=1}^{10} i \cdot a_i) + (r-j)x_j + (j-r)x_r \equiv (r-j)x_j + (j-r)x_r(\text{mod})11$.
   Στην τελευταία σχέση έχουμε ότι, αν $r \neq j$ και $x_r \neq x_j$, $(r-j)x_j + (j-r)x_r = (r-j)(x_j - x_r) \neq 0(\text{mod})11$. Οπότε ανιχνεύουμε τον αναγραμματισμό [7].

4. Επίσης ο κώδικας έχει την έξης μερική δυνατότητα για τη διόρθωση λαθών. Υποθέτουμε, όπως προηγουμένως, ότι εστάλει η (κωδικο)λέξη $\mathbf{a} = a_1a_2\cdots a_9a_{10}$ και ελήφθει η λέξη $\mathbf{x} = x_1x_2\cdots x_9x_{10}$, η οποία συμφωνεί σε όλους τους χαρακτήρες με την $\mathbf{a}$, εκτός από τον χαρακτήρα a_r, όπου αντί αυτού έχουμε τον χαρακτήρα $x_r = a_r + e$ με $e \neq 0$. Από τη σέχη $\sum_{i=1}^{10} i \cdot x_i = (\sum_{i=1}^{10} i \cdot a_i) + r \cdot e \neq 0(\text{mod})11$ βλέπουμε ότι αν γνωρίζουμε τη θέση r στην οποία επήλθε η αλλοίωση του χαρακτήρα, τότε μπορούμε να υπολογίσουμε τον σωστό χαρακτήρα a_i, αντί του $x_i = a_i + e$ που λάβαμε. Φυσικά μπορούμε αντίστροφα να υπολογίσουμε τη θέση στην οποία επήλθε η αλλοίωση αν γνωρίζουμε το e που προκάλεσε την αλλοίωση .

[7] Αν στις θέσεις που έγινε ο αναγραμματισμός οι χαρακτήρες συνέπιπταν, τότε θα είχαμε $x_r = a_j = a_r = x_j$. Ο αναγραμματισμός δεν θα ανιχνεύετο, διότι στην πραγματικότητα δεν έγινε αναγραμματισμός.

Τελειώνοντας την παράγραφο επισημαίνουμε ότι οι δύο τρόποι αποκωδικοποίησης που αναφέραμε, η αρχή της αποκωδικοποίησης μέγιστης πιθανότητας και η αρχή της αποκωδικοποίησης ως προς την πλησιέστερη λέξη, στην πραγματικότητα αποτελούν τις δύο όψεις του *ιδίου νομίσματος*.

Έστω ότι έχουμε τον δυαδικό κώδικα $\mathcal{C}$ και έναν συμμετρικό δίαυλο με πιθανότητα μετάδοσης λάθους χαρακτήρα ίση με $p < 1/2$, δηλαδή
$p(\epsilon\lambda\acute{\eta}\varphi\theta\epsilon\iota\ o\ \chi\alpha\rho\alpha\kappa\tau\acute{\eta}\rho\alpha\varsigma\ 1 \mid \epsilon\sigma\tau\acute{\alpha}\lambda\epsilon\iota\ o\ \chi\alpha\rho\alpha\kappa\tau\acute{\eta}\rho\alpha\varsigma\ 0) =$
$= p(\epsilon\lambda\acute{\eta}\varphi\theta\epsilon\iota\ o\ \chi\alpha\rho\alpha\kappa\tau\acute{\eta}\rho\alpha\varsigma\ 0 \mid \epsilon\sigma\tau\acute{\alpha}\lambda\epsilon\iota\ o\ \chi\alpha\rho\alpha\kappa\tau\acute{\eta}\rho\alpha\varsigma\ 1) = p,$
οπότε η πιθανότητα μετάδοσης σωστού χαρακτήρα είναι ίση με $1-p$, δηλαδή
$p(\epsilon\lambda\acute{\eta}\varphi\theta\epsilon\iota\ o\ \chi\alpha\rho\alpha\kappa\tau\acute{\eta}\rho\alpha\varsigma\ 0 \mid \epsilon\sigma\tau\acute{\alpha}\lambda\epsilon\iota\ o\ \chi\alpha\rho\alpha\kappa\tau\acute{\eta}\rho\alpha\varsigma\ 0) =$
$= p(\epsilon\lambda\acute{\eta}\varphi\theta\epsilon\iota\ o\ \chi\alpha\rho\alpha\kappa\tau\acute{\eta}\rho\alpha\varsigma\ 1 \mid \epsilon\sigma\tau\acute{\alpha}\lambda\epsilon\iota\ o\ \chi\alpha\rho\alpha\kappa\tau\acute{\eta}\rho\alpha\varsigma\ 1) = 1-p.$ Υποθέτουμε ότι ο δέκτης λαμβάνει τη λέξη $\mathbf{x} = x_1\, x_2 \cdots x_n$, ενώ εστάλει η λέξη
$\mathbf{c} = c_1\, c_2 \cdots c_n$. Θέλουμε να υπολογίσουμε την πιθανότητα
$p(\epsilon\lambda\acute{\eta}\varphi\theta\epsilon\iota\ \eta\ \lambda\acute{\epsilon}\xi\eta\ \mathbf{x} \mid \epsilon\sigma\tau\acute{\alpha}\lambda\epsilon\iota\ \eta\ \lambda\acute{\epsilon}\xi\eta\ \mathbf{c})$. Αν κατά τη μετάδοση υπεισήλθαν k το πλήθος λάθη (δηλαδή το διάνυσμα λάθους έχει βάρος k), τότε, σύμφωνα με την (1.2.1), έχουμε

$$p(\ \epsilon\lambda\acute{\eta}\varphi\theta\epsilon\iota\ \eta\ \ \mathbf{x}\ \mid\ \ \epsilon\sigma\tau\acute{\alpha}\lambda\epsilon\iota\ \eta\, \mathbf{c}\ ) =$$

$$= \prod_{i=1}^{n} p(\ \epsilon\lambda\acute{\eta}\varphi\theta\epsilon\iota\ o\, x_i\ \mid\ \epsilon\sigma\tau\acute{\alpha}\lambda\epsilon\iota\ o\ \ c_i) \ = \ p^k(1-p)^{n-k}$$

Επειδή $p < 1/2$, έχουμε $1-p > p$. Επομένως η προηγούμενη πιθανότητα γίνεται όσο το δυνατόν μεγαλύτερη (αρχή της μέγιστης πιθανότητας), όταν ο εκθέτης $n-k$ γίνεται όσο το δυνατόν μεγαλύτερος, δηλαδή ο k γίνεται όσο το δυνατόν μικρότερος, άρα όσο η λέξη $\mathbf{x}$ είναι πλησιέστερα στη λέξη $\mathbf{c}$ (αρχή της πλησιέστερης λέξης). Δηλαδή αποδείξαμε το εξής σημαντικό Θεώρημα.

Θεώρημα 1.3.20. *Σε ένα δυαδικό, συμμετρικό δίαυλο η αρχή της αποκωδικοποίησης μέγιστης πιθανότητας είναι η ίδια με την αρχή της αποκωδικοποίησης ως προς την πλησιέστερη λέξη.*

Παρατήρηση 1.3.21. Το θεώρημα αυτό ισχύει στη γενική περίπτωση ενός $r-$αδικού συμμετρικού δίαυλου επικοινωνίας με μόνη προϋπόθεση οι πιθανότητες μετάδοσης $p_{ij} = p(\epsilon\lambda\acute{\eta}\varphi\theta\epsilon\iota\ o\ \chi\alpha\rho\alpha\kappa\tau\acute{\eta}\rho\alpha\varsigma\ a_i \mid \epsilon\sigma\tau\acute{\alpha}\lambda\epsilon\iota\ o\ \chi\alpha\rho\alpha\kappa\tau\acute{\eta}\rho\alpha\varsigma\ a_j) = p$ να πληρούν τη σχέση $p < \frac{1}{2(r-1)}$, ούτως ώστε η πιθανότητα
$p_{ii} = p(\epsilon\lambda\acute{\eta}\varphi\theta\epsilon\iota\ o\ \chi\alpha\rho\alpha\kappa\tau\acute{\eta}\rho\alpha\varsigma\ a_i \mid \epsilon\sigma\tau\acute{\alpha}\lambda\epsilon\iota\ o\ \chi\alpha\rho\alpha\kappa\tau\acute{\eta}\rho\alpha\varsigma\ a_i) =$
$= 1-(r-1)p > 1-(r-1)\cdot\frac{1}{2(r-1)} = 1/2.$

Η απόδειξη, αν και πιο σύνθετη, είναι ακριβώς η ίδια, ως προς την ιδέα, με την προηγούμενη.

1.3.3 Ταυτόχρονη ανίχνευση και διόρθωση λαθών

Έστω ότι έχουμε έναν κώδικα $\mathcal{C}$ με ελάχιστη απόσταση $d(\mathcal{C}) = d$. Σύμφωνα με τα προηγούμενα, αν ο $\mathcal{C}$ χρησιμοποιηθεί μόνο για ανίχνευση λαθών, θα ανιχνεύει (μέχρι) $d-1$ το πλήθος λάθη. Αν χρησιμοποιθεί μόνο για διόρθωση λαθών θα διορθώνει (μέχρι) $\left[\frac{d-1}{2}\right]$ το πλήθος λάθη. Συνήθως όμως ένας κώδικας χρησιμοποιείται ταυτόχρονα και για διόρθωση λαθών και για ανίχνευση λαθών.

Η ταυτόχρονη χρήση ενός κώδικα για διόρθωση και ανίχνευση λαθών είναι " συμφέρουσα " ως προς την εξοικονόμηση ενέργειας, χρόνου, χρημάτων κ.λ.π., αλλά χρειάζεται να είμαστε προσεκτικοί ως προς τον μέγιστο αριθμό λαθών που μπορεί να ανιχνεύσει, εφόσον αυτά δεν έχουν " διορθωθεί ".
Μια αβασάνιστη σκέψη θα έλεγε ότι αν σε μια (κωδικο)λέξη έχουν υπεισέλθει περισσότερα από $\left[\frac{d-1}{2}\right]$, αλλά λιγότερα από $d-1$ το πλήθος λάθη, τότε ο κώδικας θα επισημάνει την ύπαρξη λαθών. Αυτό αποτελεί εσφαλμένη αντίληψη, όπως θα δούμε απο το εξής απλό παράδειγμα. Έστω ο δυαδικός κώδικας $\mathcal{C} = \{\,000000, 111111\,\}$, υποθέτουμε ότι αποστέλεται η (κωδικο)λέξη $\mathbf{c} = 000000$ και λαμβάνεται η λέξη $\mathbf{x} = 111100$ (έχουν υπησέλθει τέσσερα λάθη). Σύμφωνα με την αρχή αποκωδικοποίησης ως προς την πλησιέστερη λέξη, η λέξη $\mathbf{x} = 111100$ θα αποκωδικοποιηθεί (κακώς) ως η λέξη $\mathbf{b} = 111111$ και ο κώδικας **δεν** θα ανιχνεύσει το λάθος παρ'ολο που ο κώδικας ανιχνεύει (μέχρι) πέντε λάθη, αν χρησιμοποιηθεί μόνο για ανίχνευση λαθών.
Στο παράδειγμα αυτό η ελάχιστη απόσταση είναι 6, άρτιος αριθμός. Πριν προχωρήσουμε στην διατύπωση και απόδειξη ενός γενικού αποτελέσματος, ας δούμε ένα παράδειγμα ενός κώδικα με περιττή ελάχιστη απόσταση. Έστω ο δυαδικός κώδικας $\mathcal{C} = \{\,1110000, 1011111\,\}$. Ο κώδικας διορθώνει ακριβώς 2 λάθη, υποθέτουμε ότι αποστέλεται η (κωδικο)λέξη $\mathbf{c} = 1011111$ και λαμβάνεται η λέξη $\mathbf{x} = 1011000$ (έχουν υπησέλθει τρία λάθη). Σύμφωνα με την αρχή αποκωδικοποίησης ως προς την πλησιέστερη λέξη, η λέξη $\mathbf{x} = 1011000$ θα αποκωδικοποιηθεί (κακώς) ως η λέξη $\mathbf{b} = 1110000$ και ο κώδικας **δεν** θα ανιχνεύσει το λάθος παρ'ολο που ο κώδικας ανιχνεύει (μέχρι) τέσσερα λάθη, αν χρησιμοποιηθεί μόνο για ανίχνευση λαθών. Μάλιστα δε θα μπορούσαμε να πούμε ότι ανιχνεύει τόσα λάθη όσα διορθώνει.

Θεώρημα 1.3.22. *Έστω ο κώδικας $\mathcal{C}$ με ελάχιστη απόσταση $d(\mathcal{C}) = d$.*

1. *Υποθέτουμε ότι $d = 2\lambda + 2$. Αν ο κώδικας χρησιμοποιθεί για διόρθωση και ανίχνευση λαθών, τότε διορθώνει ακριβώς λ λάθη και ανιχνεύει $\lambda + 1$ λάθη, αλλά υπάρχουν διανύσματα λάθους με βάρος μεγαλύτερο από $\lambda + 1$ τα οποία δεν ανιχνεύονται.*

2. *Υποθέτουμε ότι* $d = 2\lambda+1$. *Αν ο κώδικας χρησιμοποιθεί για διόρθωση και ανίχνευση λαθών, τότε διορθώνει ακριβώς* λ *λάθη και δεν ανιχνεύει* $\lambda+1$ *λάθη, δηλαδή υπάρχουν διανύσματα λάθους με βάρος* $\lambda+1$ *τα οποία δεν ανιχνεύονται.*

Απόδειξη. Υποθέτουμε ότι η ελάχιστη απόσταση του κώδικα είναι άρτια της μορφής $d = 2\lambda + 2$. Από τα προηγούμενα (1.3.17) έχουμε ότι ο κώδικας διορθώνει ακριβώς λ το πλήθος λάθη. Έστω τώρα ότι εστάλη η (κωδικο)λέξη $\mathbf{c}$ και ελήφθει η λέξη $\mathbf{x}$ στην οποία έχουν υπεισέλθει $\lambda + 1$ λάθη. Κάθε (κωδικο)λέξη απέχει από την $\mathbf{x}$ απόσταση τουλάχιστον ίση με $\lambda + 1$. Πράγματι, αν υπήρχε μια (κωδικο)λέξη $\mathbf{d}$ με $d(\mathbf{x}, \mathbf{d}) \leq \lambda$, τότε θα είχαμε $d(\mathbf{c}, \mathbf{d}) \leq d(\mathbf{c}, \mathbf{x}) + d(\mathbf{x}, \mathbf{d}) \leq \lambda + 1 + \lambda < 2\lambda + 2 = d$, άτοπο. Επομένως η $\mathbf{x}$ δεν αποκωδικοποιείται και ανιχνεύεται το λάθος.
Έστω, τώρα δύο (κωδικο)λέξεις $\mathbf{c}$ και $\mathbf{d}$ με απόσταση ίση με την ελάχιστη απόσταση του κώδικα. Επειδή η ελάχιστη απόσταση είναι ίση με $d = 2\lambda+2$ υπάρχει τουλάχιστον μια λέξη $\mathbf{x}$ η οποία απέχει από την $\mathbf{c}$ απόσταση $\lambda + 2$ και από την $\mathbf{d}$ απόσταση λ (γιατί υπάρχει τέτοια λέξη;). Υποθέτουμε ότι εστάλει η λέξη $\mathbf{c}$, υπεισήλθαν $\lambda + 2$ το πλήθος λάθη και αντ΄ αυτής λάβαμε τη λέξη $\mathbf{x}$. Σύμφωνα με την αρχή αποκωδικοποίησης ως προς την πλησιέστερη λέξη, η λέξη $\mathbf{x}$ θα αποκωδικοποιηθεί (κακώς) ως η λέξη $\mathbf{d}$ και ο κώδικας **δεν** θα ανιχνεύσει το λάθος παρ'ολο που ο κώδικας ανιχνεύει (μέχρι) $2\lambda + 1$ λάθη, αν χρησιμοποιηθεί μόνο για ανίχνευση λαθών.

Στην περίπτωση που η ελάχιστη απόσταση του κώδικα είναι περιττή της μορφής $d = 2\lambda + 1$ πάλι ο κώδικας διορθώνει ακριβώς λ το πλήθος λάθη. Αν οι (κωδικο)λέξεις $\mathbf{c}$ και $\mathbf{d}$ απέχουν απόσταση ίση με την ελάχιστη απόσταση του κώδικα, τότε υπάρχει τουλάχιστον μια λέξη $\mathbf{x}$ η οποία απέχει από την την $\mathbf{c}$ απόσταση $\lambda+1$ και από την $\mathbf{d}$ απόσταση λ (γιατί υπάρχει τέτοια λέξη;). Υποθέτουμε ότι εστάλει η λέξη $\mathbf{c}$, υπεισήλθαν $\lambda + 1$ το πλήθος λάθη και αντ΄ αυτής λάβαμε τη λέξη $\mathbf{x}$. Σύμφωνα με την αρχή αποκωδικοποίησης ως προς την πλησιέστερη λέξη, η λέξη $\mathbf{x}$ θα αποκωδικοποιηθεί (κακώς) ως η λέξη $\mathbf{d}$ και ο κώδικας **δεν** θα ανιχνεύσει το λάθος παρ'ολο που ο κώδικας ανιχνεύει (μέχρι) 2λ λάθη, αν χρησιμοποιηθεί μόνο για ανίχνευση λαθών.

□

1.3.4 Ασκήσεις

1. Υποθέτουμε ότι έχουμε τον δυαδικό κώδικα $\mathcal{C} = \{\, 0000, 1111 \,\}$ και για την μετάδοση χρησιμοποιούμε έναν συμμετρικό δίαυλο επικοινωνίας με πιθανότητα μετάδοσης $p = 0,01$. Αν λάβαμε τις λέξεις 0000, 0010, 1010, εφαρμόστε την αρχή αποκωδικοποίησης μεγίστης πιθανότητας για να απο-

κωδικοποιήσετε αυτές τις λέξεις.
Όμοια για τον κώδικα $\mathcal{C} = \{\,000,\, 001,\, 111\,\}$ και για τις ληφθείσες λέξεις 010, 101, 110.

2. Υποθέτουμε ότι έχουμε τον κώδικα $\mathcal{C} = \{\,000,\, 001,\, 111\,\}$ και τις ληφθείσες λέξεις 010, 101, 110 μέσω ενός δυαδικού διαύλου επικοινωνίας με πιθανότητες μετάδοσης $p(\,\textit{ελήφθει το}\, 0 \mid \textit{εστάλει το}\ 0) = 3/4$ και $p(\,\textit{ελήφθει το}\, 1 \mid \textit{εστάλει το}\ 1) = 7/8$. Εφαρμόστε την αρχή αποκωδικοποίησης μεγίστης πιθανότητας για να αποκωδικοποιήσετε αυτές τις λέξεις.

3. Εξετάστε αν υπάρχουν δυαδικοί κώδικες που να διορθώνουν ένα λάθος με παραμέτρους $(5,\, 6),\ (6,\, 9)$.
Εξετάστε αν υπάρχουν δυαδικοί κώδικες που να διορθώνουν δύο λάθη με παραμέτρους $(8,\ 4),\ (8,\ 5)$.

4. Δείξτε ότι σε έναν τριαδικό κώδικα με παραμέτρους $(3,\, M,\, 2)$ πρέπει να ισχύει $M \leq 9$.
Κατασκευάστε έναν τριαδικό $(3,\, 9,\, 2)$ κώδικα.

5. Μα κατασκευάσετε, ή να αποδείξετε ότι δεν υπάρχουν, δυαδικοί κώδικες με παραμέτρους $(8,2,8),\ (8,3,8),\ (3,9,1),\ (4,8,2),\ (5,3,4)$.

6. Έστω ένας κώδικας, του οποίου τα στοιχεία είναι όλες οι λέξεις από το $\mathbb{Z}_2^n$ με άρτιο το πλήθος χαρακτήρες ίσον με 1. Να υπολογίσετε το μέγεθος και την ελάχιστη απόσταση αυτού του κώδικα.

7. Να υπολογίσετε την πιθανότητα σωστής αποκωδικοποίησης για τον κώδικα $\mathcal{C} = \{\,00000,\, 11111\,\}$, όπου η αποστολή γίνεται μέσω ενός δυαδικού συμμετρικού διαύλου επικοινωνίας με πιθανότητα μετάδοσης ίση με $p = 0,001$.

8. Έστω ένας κώδικας $\mathcal{C}$ με παραμέτρους $(15,\, 2^{11},\, 3)$. Να υπολογίσετε την μέγιστη πιθανότητα σωστής αποκωδικοποίησης, όταν για την μετάδοση χρησιμοποιείται ένας δυαδικός συμμετρικός δίαυλος επικοινωνίας με πιθανότητα μετάδοσης ίση με p.

9. Έστω ένας κώδικας $\mathcal{C}$ με ελάχιστη απόσταση ίση με $d(\mathcal{C}) \geq 2\lambda + \mu + 1$. Δείξτε ότι ο $\mathcal{C}$ μπορεί ταυτόχρονα να διορθώνει λ και να ανιχνεύει μ το πλήθος λάθη.

10. Οι λέξεις $0\,8218\,26 - 8\,Q$, $- - 87\,94703\,3$ αποτελούν στοιχεία του κώδικα ISBN, αλλά κατά τη διάρκεια της μετάδοσης "χάθηκαν" ορισμένοι χαρακτήρες. Μπορείτε να εκτιμήσετε τους χαρακτήρες που χάθηκαν;

11. Έστω ο $10-$κώδικας $\mathcal{C}$, του οποίου τα στοιχεία είναι λέξεις μήκους δέκα και το άθροισμα των χαρακτήρων μιας λέξης είναι πολλαπλάσιο του 11. Δηλαδή $\mathcal{C} = \{ x_1x_2 \cdots x_{10} \mid x_i = 0, 1, \ldots, 9, \ \sum_{i=1}^{10} x_i \equiv 0 \mathrm{mod} 11 \}$. Δείξτε ο $\mathcal{C}$ ανιχνεύει ένα λάθος.
Σε τι μειονεκτεί έναντι του κώδικα ISBN;

1.4 Κώδικες που προέρχονται από άλλους κώδικες

Έστω ένας $r-$αδικός (n, M, d) κώδικας. Όπως έχουμε παρατηρήσει κάθε μία από τις παραμέτρους n, M και d έχει τη σημασία της ως προς την *αποτελεσματικότητα* του κώδικα. Το μήκος n των κωδικολέξεων έχει σχέση με το *μέγεθος* της πληροφορίας που μπορεί να μεταδοθεί μέσω μιας κωδικολέξης, αλλά υπόκειται σε *φυσικούς* περιορισμούς, όπως είναι ο χρόνος που απαιτείται για τη μετάδοση μιας λέξης ή η απαιτούμενη μνήμη για την αποθήκευση μιας λέξης. Το πλήθος M των *διαθέσιμων* κωδικολέξεων έχει σχέση με το *πλήθος* των πληροφοριών που μπορούν να μεταδοθούν μέσω του κώδικα. Η ελάχιστη απόσταση d έχει σχέση με την δυνατότητα που έχει ο κώδικας να ανιχνεύει και να διορθώνει λάθη, αλλά έχει άμεση σχέση τόσο με το μήκος του κώδικα, όσο και με το μέγεθός του. Οι τρεις αυτές παράμετροι βρίσκονται *αντιμέτωπες* και ο προσδιορισμός του *καταλληλότερου* κώδικα εξαρτάται τόσο από τη φύση των μεταδιδόμενων μυνημάτων, όσο και από τα διαθέσιμα μέσα.

1.4.1 Μερικές περιπτώσεις "μετασκευής " κωδίκων

Στην παράγραφο αυτή θα δούμε, σε πολύ λίγες περιπτώσεις, πώς από ένα δεδομένο κώδικα μπορούμε να κατασκευάσουμε ένα *βελτιωμένο* κώδικα, ο οποίος να πληροί ορισμένες προϋποθέσεις που δεν πληροί ο προηγούμενος κώδικας.

Σημείωση: Η έκφραση βελτιωμένος κώδικας είναι σχετική και επιδέχεται πολλές ερμηνείες, για το λόγο αυτό στα επόμενα, τις περισσότερες φορές, θα γίνεται προσπάθεια κατά περίπτωση να διευκρινίζεται ως προς τι έγκειται η βελτίωση.

Ισοδύναμοι κώδικες

Όπως σε όλους τους κλάδους των Μαθηματικών η έννοια της ισοδυναμίας είναι θεμελιώδης, έτσι και στη θεωρία κωδίκων η έννοια των ισοδυνάμων κωδίκων είναι πολύ βασική. Δεδομένου ότι ισοδύναμοι κώδικες είναι στην πραγματικότητα " ίδιοι " όσον αφορά το μήκος, το μέγεθος, την ελάχιστη απόσταση και συνεπώς την ικανότητα να ανιχνεύουν/διορθώνουν λάθη.

Ορισμός 1.4.1. *Έστω $\mathcal{C}$ ένας (n, M) κώδικας επί του αλφάβητου $\mathbb{A}$. Θεωρούμε την εξής διαδικασία μετασχηματισμού του $\mathcal{C}$.*

1. Για μια δεδομένη μετάθεση σ στα σύμβολα $\{1, 2, \ldots, n\}$ αντικαθιστούμε κάθε (κωδικο)λέξη $\mathbf{c} = c_1c_2 \cdots c_n$ με την λέξη $c_{\sigma(1)}c_{\sigma(2)} \cdots c_{\sigma(n)}$, οπότε προκύπτει ένας νέος κώδικας, έστω $\mathcal{D}$.

2. Σε κάθε θέση i των χαρακτήρων (κάθε)μιας (κωδικο)λέξης εφαρμόζουμε μια μετάθεση π_i στους χαρακτήρες του αλφάβητου $\mathbb{A}$, οπότε μια (κωδικο)λέξη, έστω $\mathbf{d} = d_1d_2 \cdots d_n$ την αντικαθιστούμε με την λέξη $\pi_1(d_1)\pi_2(d_2) \cdots \pi_n(d_n)$. Συνεπώς προκύπτει ένας νέος κώδικας, έστω $\mathcal{F}$.

Ο κώδικας που προκύπτει σύμφωνα με την παραπάνω διαδικασία ονομάζεται **ισοδύναμος** *προς τον κώδικα $\mathcal{C}$. .*

Επειδή κάθε μετάθεση είναι μια αντιστρέψιμη απεικόνιση, προφανώς, αν ο κώδικας $\mathcal{E}$ είναι ισοδύναμος προς τον κώδικα $\mathcal{C}$, τότε και ο κώδικας $\mathcal{C}$ είναι ισοδύναμος προς τον κώδικα $\mathcal{E}$. Επομένως στο εξής μπορούμε να λέμε οτι οι δύο κώδικες είναι ισοδύναμοι χωρίς διάκριση.

Μάλιστα μπορούμε να αποδείξουμε ότι στο σύνολο των κωδίκων επί ενός αλφάβητου $\mathbb{A}$ με σταθερό μήκος η ισοδυναμία κωδίκων αποτελεί σχέση ισοδυναμίας. (γιατί;)

Το ότι ισοδύναμοι κώδικες είναι ίδιοι, όπως προείπαμε, φαίνεται από το ακόλουθο θεώρημα.

Θεώρημα 1.4.2. *Ισοδύναμοι κώδικες έχουν τις ίδιες παραμέτρους (μήκος, μέγεθος και ελάχιστη απόσταση).*

Απόδειξη. Η απόδειξη αποτελεί μια απλή εφαρμογή του ορισμού και αφήνεται ως άσκηση.

□

Παράδειγμα 1.4.3. Έστω ο τριαδικός κώδικας $\mathcal{C} = \{120, 102, 210, 110, 212\}$. Επιλέγουμε τις μεταθέσεις $\pi_1 : (0 \to 1, 1 \to 0, 2 \to 2)$, $\pi_2 : (0 \to 2, 1 \to 1, 2 \to 0)$, $\pi_3 = (0 \to 0, 1 \to 1, 2 \to 2)$ και τις εφαρμόζουμε στα στοιχεία του κώδικα σύμφωνα με το δεύτερο βήμα της παραπάνω διαδικασίας. Δεν είναι δύσκολο να δούμε ότι ο ισοδύναμος κώδικας που προκύπτει είναι ο κώδικας $\mathcal{D} = \{000, 022, 210, 010, 212\}$.

Στο προηγούμενο παράδειγμα βλέπουμε ότι στον κώδικα $\mathcal{D}$ υπάρχει η (κωδικο)λέξη 000, όπου όλοι οι χαρακτήρες είναι ίδιοι. Αυτό μπορούμε να το πετύχουμε σε οποιονδήποτε κώδικα. Συγκεκριμένα ισχύει η εξής σημαντική πρόταση.

Πρόταση 1.4.4. *Έστω $\mathcal{C}$ ένας (n, M) κώδικας επί του αλφάβητου $\mathbb{A}$. Επιλέγουμε και σταθεροποιούμε ένα γράμμα $a \in \mathbb{A}$, υπάρχει κώδικας ισοδύναμος με τον κώδικα $\mathcal{C}$, ο οποίος περιέχει την (κωδικο)λέξη $\mathbf{a} = (a, a, \ldots, a)$*

Απόδειξη. Η απόδειξη είναι απλή και αφήνεται ως άσκηση, αρκεί να προσέξουμε καλά το προηγούμενο παράδειγμα.

□

Εδώ είναι σκόπιμο να αναφέρουμε ότι, αν θέλουμε να εφαρμόσουμε το πρώτο βήμα μετασχηματισμού ενός κώδικα σε έναν ισοδύναμό του, μπορούμε να ενεργήσουμε ως εξής·
Έστω σ μια μετάθεση των στοιχείων του συνόλου $\{1, 2, \ldots, n\}$ και I_n ο ταυτοτικός $n \times n$ πίνακας. Στις γραμμές του I_n εφαρμόζουμε την μετάθεση σ. Για παράδειγμα, αν $\sigma(i) = j_i$, μεταθέτουμε την i-γραμμή στη θέση της j_i-γραμμής κ.ο.κ.. Οπότε προκύπτει ένας $n \times n$ πίνακας P_σ, όπου στις (j_i, i) θέσεις, για $i = 1, 2, \ldots, n$ έχει 1 και σε όλες τις υπόλοιπες 0. Ο πίνακας P_σ ονομάζεται συνήθως πίνακας **πίνακας μετάθεση** (ως προς τη μετάθεση σ). Υποθέτουμε τώρα ότι έχουμε την (κωδικο)λέξη $\mathbf{c} = c_1c_2\cdots c_n$, δεν είναι δύσκολο να δούμε ότι αν θεωρήσουμε την $\mathbf{c}$ σαν έναν πίνακα γραμμή και κάνουμε τον πολλαπλασιασμό $\mathbf{c}P_\sigma$, τότε έχουμε σαν αποτέλεσμα $\mathbf{c}P_\sigma = c_{\sigma(1)}c_{\sigma(2)}\cdots c_{\sigma(n)}$. Δηλαδή έχουμε αποδείξει την εξής πρόταση.

Πρόταση 1.4.5. *Για κάθε μετάθεση σ και κάθε κώδικα $\mathcal{C}$ μπορούμε να κατασκευάσουμε έναν ισοδύναμο κώδικα $\mathcal{C}_\sigma = \{\mathbf{c}P_\sigma \mid \mathbf{c} \in \mathcal{C}\}$.*

Θα δούμε τη χρησιμότητα αυτής της πρότασης αργότερα, όταν ασχοληθούμε με γραμμικούς κώδικες.

Θα τελειώσουμε με τους ισοδύναμους κώδικες αναφέροντας ένα παράδειγμα μοναδικότητας κωδίκων (αν θεωρήσουμε ότι ισοδύναμοι είναι ίδιοι σύμφωνα με το Θεώρημα 1.4.2).

Θεώρημα 1.4.6. *Κάθε δυαδικός $(24, 4096, 8)$-κώδικας είναι ισοδύναμος με τον $\mathcal{G}_{24}$ Golay κώδικα.*

Απόδειξη. Η απόδειξη απαιτεί γνώσεις από τους γραμμικούς κώδικες.

Βλέπε τη σχετική συζήτηση στην Παράγραφο 3.3 και το Θεώρημα 3.3.4.

□

Επέκταση ενός κώδικα

Έστω $\mathcal{C}$ ένας κώδικας, μπορούμε να αυξήσουμε το μήκος κάθε (κωδικο)λέξης παρεμβάλοντας, π. χ. μεταξύ της i και $i+1$ συντεταγμένης, έναν χαρακτήρα. Τότε προκύπτει ένας νέος κώδικας $\hat{\mathcal{C}}$ με το ίδιο πλήθος στοιχείων, ο οποίος ονομάζεται **επέκταση** του $\mathcal{C}$.

Η κατάσταση που μόλις περιγράψαμε είναι τελείως γενική καθότι η αυθαιρεσία στην παρεμβολή επιπλέον χαρακτήρων δεν προσφέρει στη βελτίωση του αρχικού

κώδικα. Στην πράξη έχει επικρατήσει ο επιπλέον χαρακτήρας να επισυνάπτεται στο τέλος κάθε (κωδικο)λέξης, να μην είναι τυχαίος, αλλά να εξαρτάται από τους προηγούμενους χαρακτήρες. Συγκεκριμένα μια επέκταση ενός p- αδικού κώδικα $\mathcal{C}$ μήκους n είναι ο κώδικας $\hat{\mathcal{C}} = \{\, c_1c_2\cdots c_nc_{n+1} \mid c_1c_2\cdots c_n \in \mathcal{C} \text{ και } \sum_{i=1}^{n+1} c_i = 0 \,\}$.

Ο επιπλέον χαρακτήρας c_{n+1} που επισυνάπεται ονομάζεται **ψηφίο ελέγχου ισοτιμίας** .

Προφανώς ο κώδικας $\hat{\mathcal{C}}$ έχει μήκος ίσο με $n+1$, μέγεθος ίσο με το μέγεθος του $\mathcal{C}$ και ελάχιστη απόσταση ίση με d ή $d+1$, όπου d είναι η ελάχιστη απόσταση του κώδικα $\mathcal{C}$.

Γενικά, ένας $p-$αδικός κώδικας με την ιδιότητα το άθροισμα των χαρακτήρων σε κάθε (κωδικο)λέξη να είναι ίσον με μηδέν όνομάζεται κώδικας **μηδενικού αθροίσματος** .

Παραδείγματα 1.4.7. 1. Έστω ο δυαδικός κώδικας $\mathcal{C} = \{\, 00, 01, 10, 11 \,\}$, προσθέτοντας ένα ψηφίο ελέγχου ισοτιμίας η επέκταση του $\mathcal{C}$ είναι ο κώδικας $\hat{\mathcal{C}} = \{\, 000, 011, 101, 110 \,\}$, ο οποίος έχει ελάχιστη απόσταση δύο, ενώ ο $\mathcal{C}$ έχει ελάχιστη απόσταση ένα.

2. Έστω ο τριαδικός κώδικας $\mathcal{C} = \{\, 102, 210, 021 \,\}$, η επέκτασή του είναι ο κώδικας $\hat{\mathcal{C}} = \{\, 1020, 2100, 0210 \,\}$, ο οποίος έχει ελάχιστη απόσταση τρία, εδώ όμως και ο $\mathcal{C}$ έχει ελάχιστη απόσταση τρία.

Για δυαδικούς κώδικες ισχύει η πρόταση.

Πρόταση 1.4.8. *Έστω $\mathcal{C}$ ένας δυαδικός κώδικας. Η ελάχιστη απόσταση της επέκτασης $\hat{\mathcal{C}}$ είναι πάντα άρτια. Επομένως ο $\hat{\mathcal{C}}$ διορθώνει τόσα λάθη όσα και ο αρχικός, αλλά ενδέχεται να ανιχνεύει ένα επιπλέον λάθος απ' ότι ο αρχικός κώδικας.*

Απόδειξη. Η απόδειξη είναι απλή, αρκεί να παρατηρήσουμε ότι στην επέκταση όλες οι λέξεις είναι αρτίου βάρους και να εφαρμόσουμε τα Θεωρήματα 1.3.14 και 1.3.16 .

□

Σύμπτυξη ενός κώδικα

Η αντίστροφη διαδικασία της επέκτασης ενός κώδικα είναι η **σύμπτυξη** , όπου διαγράφουμε από όλες τις (κωδικο)λέξεις το χαρακτήρα σε μια συγκεκριμένη συντεταγμένη. Προφανώς, αν ο αρχικός κώδικας είναι ένας (n, M, d) κώδικας, ο συνεπτυγμένος κώδικας είναι ένας $(n-1, M, \bar{d})$ κώδικας με $\bar{d} = d$ ή $d-1$

Η πλέον συνηθισμένη περίπτωση σύμπτυξης κώδικα είναι, όταν σε όλες τις (κωδικο)λέξεις σε μια συγκεκριμένη θέση εμφανίζεται ο ίδιος χαρακτήρας. Τότε ο χαρακτήρας αυτός **δεν** προσφέρει τίποτε στην μετάδοση πληροφοριών, οπότε συμπτύσσουμε τον κώδικα ως προς αυτή τη συντεταγμένη και λαμβάνουμε (ακριβώς) τον ίδιο κώδικα, αλλά σε *οικονομικότερη* μορφή. [8]

Με τη βοήθεια των διαδικασίων επέκτασης/σύμπτυξης ενός κώδικα μπορούμε να αποδείξουμε το εξής Θεώρημα.

Θεώρημα 1.4.9. *Υπάρχουν δυαδικοί* $(n, M, 2t+1)$ *κώδικες αν και μόνο αν υπάρχουν* $(n+1, M, 2t+2)$ *δυαδικοί κώδικες.*

Απόδειξη. Υποθέτουμε ότι έχουμε έναν δυαδικό $(n, M, 2t+1)$ κώδικα. Τον επεκτείνουμε προσθέτοντας ένα ψηφίο ελέγχου ισοτιμίας. Από την Πρόταση 1.4.8 έχουμε ότι η ελάχιστη απόσταση, του κώδικα που προκύπτει, είναι άρτια. Άρα έχουμε έναν $(n+1, M, 2t+2)$ κώδικα.

Αντίστροφα, υποθέτουμε ότι έχουμε έναν $(n+1, M, 2t+2)$ κώδικα. Έστω $\mathbf{c}, \mathbf{d}$ δύο (κωδικο)λέξεις του, οι οποίες απέχουν μεταξύ τους απόσταση ίση με την ελάχιστη απόσταση του κώδικα ($d(\mathbf{c}, \mathbf{d}) = 2t+2$),επιλέγουμε μια συντεταγμένη στην οποία οι δύο λέξεις διαφέρουν και συμπτύσουμε ως προς αυτή τη συντεταγμένη. Ο κώδικας που προκύπτει είναι ένας $(n, M, 2t+1)$ κώδικας.

□

(Αποδελτίωση) Σμίκρυνση/Αύξηση ενός κώδικα

Ορισμένες φορές από έναν κώδικα διαγράφουμε ορισμένες (κωδικο)λέξεις, οπότε προκύπτει ένας νέος (υπο)κώδικας. Ο νέος κώδικας έχει το ίδιο μήκος με τον αρχικό κώδικα, αλλά μικρότερο μέγεθος, επομένως *φτωχώτερος* ως προς την μετάδοση πληροφοριών. Η ελάχιστη όμως απόσταση είναι μεγαλύτερη ή ίση από την ελάχιστη απόσταση του αρχικού κώδικα.

Η αντίστροφη διαδικασία, όπου σε έναν κώδικα επισυνάπτουμε νέες (κωδικο)λέξεις οδηγεί σε **αύξηση** του κώδικα και ο νέος κώδικας ονομάζεται **επαυξημένος** .

Παρατηρήσεις 1.4.10. 1. Η διαγραφή ορισμένων (κωδικο)λέξεων για να πετύχουμε μια σμίκρυνση ενός κώδικα (αντίστοιχα η προσθήκη λέξεων για να πετύχουμε μια αύξηση) δεν γίνεται τυχαία αλλά βάσει ορισμένων κανόνων. Αργότερα θα μας δοθεί η ευκαιρία να μελετήσουμε διαδικασίες σμίκρυνσης/αύξησης κωδίκων.

[8] Για το λόγο αυτό πολλοί στον ορισμό του κώδικα απαιτούν στις (κωδικο)λέξεις να μην υπάρχει κοινή συντεταγμένη

2. Τις περισσότερες φορές σε έναν κώδικα μια σμίκρυνση ακολουθείται από μια σύμπτυξη. Συγκεκριμένα σε έναν κώδικα κρατάμε όλες τις (κωδικο)λέξεις που έχουν μια κοινή συντεταγμένη και διαγράφουμε τις υπόλοιπες. Κατόπιν συμπτύσουμε τον (νέο) κώδικα διαγράφοντας την κοινή συντεταγμένη. Η όλη διαδικασία ονομάζεται **συμπύκνωση** .
   Για παράδειγμα, έστω ο κώδικας $\mathcal{C} = \{\, 0000, 0110, 1010, 0011, 1110 \,\}$, σε πρώτη φάση κάνουμε μια σμίκρυνση διαγράφοντας τις λέξεις 1010 και 1110. Οι εναπομείναντες λέξεις έχουν όλες στην πρώτη συντεταγμένη το μηδέν, οπότε το διαγράφουμε και έχουμε σαν τελικό αποτέλεσμα τον συμπυκνωμένο κώδικα $\mathcal{D} = \{\, 000, 110, 011 \,\}$.

Θα περιγράψουμε μια συνηθισμένη αύξηση σε δυαδικούς κώδικες.

Κατ' αρχήν έστω $\mathbf{c}$ μια δυαδική λέξη μήκους n ($\mathbf{c} \in \mathbb{Z}_2^n$). Το **συμπλήρωμά** της $\mathbf{c}^c$ είναι μια λέξη μήκους n που προκύπτει από την $\mathbf{c}$ αν μετατρέψουμε τα 0 σε 1 και τα 1 σε 0. Δηλαδή το συμπλήρωμα της $\mathbf{c} = 10011$ είναι $\mathbf{c}^c = 01100$. Προφανώς δύο λέξεις $\mathbf{c}$ και $\mathbf{d}$ είναι η μια συμπλήρωμα της άλλης αν και μόνο αν $\mathbf{c} + \mathbf{d} = \mathbf{1}$, όπου $\mathbf{1} = 11\cdots1$. Δηλαδή $\mathbf{c}^c = \mathbf{c} + \mathbf{1}$.
Έστω τώρα $\mathcal{C}$ ένας δυαδικός κώδικας μήκους n και $\mathcal{C}^c$ ο συμπληρωματικός του, δηλαδή $\mathcal{C}^c = \{\, \mathbf{c}^c \mid \mathbf{c} \in \mathcal{C} \,\}$. Το σύνολο $\mathcal{C} \cup \mathcal{C}^c$ αποτελεί μια αύξηση του κώδικα $\mathcal{C}$ (και του $\mathcal{C}^c$). Ας προσπαθήσουμε να υπολογίσουμε την ελάχιστη απόσταση του $\mathcal{C} \cup \mathcal{C}^c$.

Μια πρώτη παρατήρηση είναι ότι $d(\mathcal{C}) = d(\mathcal{C}^c)$ και για $\mathbf{c}, \mathbf{d} \in \mathbb{Z}_2^n$ ισχύει $d(\mathbf{c}, \mathbf{d}^c) = n - d(\mathbf{c}, \mathbf{d})$ (γιατί;)
Από τον ορισμό της ελάχιστης απόστασης έχουμε
$d(\mathcal{C} \cup \mathcal{C}^c) = min\{\, d(\mathcal{C}), d(\mathcal{C}^c), min\{\, d(\mathbf{c}, \mathbf{d}), \mathbf{c} \in \mathcal{C}, \mathbf{d} \in \mathcal{C}^c \,\} \,\}$.
Αλλά $min\{\, d(\mathbf{c}, \mathbf{d}), \mathbf{c} \in \mathcal{C}, \mathbf{d} \in \mathcal{C}^c \,\} = min\{\, d(\mathbf{c}, \mathbf{d}^c), \mathbf{c}, \mathbf{d} \in \mathcal{C} \,\} =$
(βάσει της προηγούμενης παρατήρησης) $= min\{\, n - d(\mathbf{c}, \mathbf{d}), \mathbf{c}, \mathbf{d} \in \mathcal{C} \,\} = n - max\{\, d(\mathbf{c}, \mathbf{d}), \mathbf{c}, \mathbf{d} \in \mathcal{C} \,\}$. Επομένως
$d(\mathcal{C} \cup \mathcal{C}^c) = min\{\, d(\mathcal{C}), n - max\{\, d(\mathbf{c}, \mathbf{d}), \mathbf{c}, \mathbf{d} \in \mathcal{C} \,\} \,\}$.

Στα επόμενα, όταν ασχοληθούμε με γραμμικούς κώδικες θα επανέλθουμε στο παράδειγμα αυτό (βλέπε Πρόταση 2.1.4).

Στο παράδειγμα 1.3.19 είχαμε ασχοληθεί με το γνωστό κώδικα **ISBN**. Εδώ θα δούμε πώς ο κώδικας αυτός μπορεί να προέλθει σαν σμίκρυνση ενός άλλου κώδικα.
Έστω $\mathcal{C} = \{\, \mathbf{c} = x_1x_2\cdots x_{10} \in \mathbb{Z}_{11}^{10} \mid x_{10} = x_1 + 2x_2 + 3x_3 + \cdots + 9x_9 \,\}$. Δεν είναι δύσκολο να αποδείξουμε ότι ο $\mathcal{C}$ είναι ένας $(\,10, 11^9, 2\,)$ κώδικας (γιατί;). Μάλιστα μπορούμε να αποδείξουμε ότι ο $\mathcal{C}$ είναι διανυσματικός χώρος επί του σώματος $\mathbb{Z}_{11}$ (αποδείξτε το!) με διάσταση 9. Από τον κώδικα αυτό διαγράφουμε όλες τις (κωδικο)λέξεις στις οποίες σε μια από τις θέσεις $i = 1, 2, \ldots, 9$ εμφανίζεται ¨10¨, ενώ επιτρέπεται στην τελευταία θέση να εμφανίζεται το ¨10¨,

οπότε προκύπτει ένας κώδικας, έστω $\mathcal{E}$. Δηλαδή $\mathcal{E} = \{\, \mathbf{c} = x_1x_2\cdots x_{10} \in \mathcal{C} \mid x_1, x_2 \ldots, x_9 \neq 10 \,\}$. Επειδή ο χαρακτήρας "10' είναι διψήφιος, προς αποφυγήν σύγχυσης, συμφωνούμε να τον συμβολίζουμε με "X". Ο κώδικας $\mathcal{E}$ είναι ο γνωστός κώδικας **ISBN** (γιατί;)

Επαναληπτικοί κώδικες

Πολλές φορές, όταν μεταδίδουμε ένα μήνυμα, για να αισθανθούμε *περισσότερο βέβαιοι* ότι ο παραλήπτης θα είναι σε θέση να αποκωδικοποιήσει το μήνυμα σωστά, επαναλαμβάνουμε κάθε (κωδικο)λέξη περισσότερες φορές. Για παράδειγμα, ας υποθέσουμε ότι θέλουμε να αποστείλουμε την (κωδικο)λέξη 1011. Αντ' αυτής αποστέλλουμε, επαναληπτικά, την λέξη 1011 1011 1011 (σκόπιμα στη γραφή παρεμβάλαμε κενά), οπότε αν έχει υπεισέλθει μόνο ένα λάθος αυτό θα βρίσκεται σε μία από τις τρείς (υπο)λέξεις. Οι άλλες δύο (υπο)λέξεις είναι οι ίδιες και επομένως το λάθος εύκολα εντοπίζεται και διορθώνεται. Προφανώς αν θέλουμε να διορθώσουμε δύο λάθη, τότε κάθε (κωδικο)λέξη κατά την αποστολή της πρέπει να επαναλαμβάνεται πέντε φορές. Γενικά, αν θέλουμε, με αυτό τον τρόπο, να διορθώνουμε λ το πλήθος λάθη, κάθε (κωδικο)λέξη κατά την αποστολή της πρέπει να επαναλαμβάνεται $2\lambda + 1$ φορές.

Ορισμός 1.4.11. *Έστω $\mathcal{C}$ ένας (n, M, d) κώδικας και k ένας θετικός ακέραιος. Ο κώδικας $\mathcal{C}_k = \{\, \underbrace{\mathbf{cc}\cdots\mathbf{c}}_{k-\text{φορές}} \mid \mathbf{c} \in \mathcal{C} \,\}$ λέγεται k-επαναληπτικός κώδικας του $\mathcal{C}$.*

Προφανώς ο κώδικας $\mathcal{C}_k$ έχει μήκος $k \cdot n$, μέγεθος M και ελάχιστη απόσταση $k \cdot d$.

Η πλέον συνηθισμένη περίπτωση επαναληπτικού κώδικα είναι η εξής. Έστω p ένας πρώτος αριθμός (ή γενικότερα δύναμη ενός πρώτου αριθμού) και k ένας θετικός ακέραιος. Ο κώδικας $\mathcal{R}_p(k) = \{\, \underbrace{00\cdots0}_{k-\text{φορές}}, \underbrace{11\cdots1}_{k-\text{φορές}}, \ldots, \underbrace{p-1\,p-1\cdots p-1}_{k-\text{φορές}} \,\}$ είναι ένας $p-$αδικός k-επαναληπτικός κώδικας. (Ποίου κώδικα είναι επαναληπτικός;) [9]

Παρατήρηση. Ένας επαναληπτικός κώδικας δεν είναι πλουσιώτερος του κώδικα από τον οποίο προέρχεται (και οι δύο έχουν το ίδιο μέγεθος), αλλά έχει την δυνατότητα να διορθώνει πολύ περισσότερα λάθη. Η δυνατότητα αυτή στην πράξη συνεκτιμάται με το γεγονός ότι το μήκος του είναι πολλαπλάσιο από το αντίστοιχο μήκος του αρχικού κώδικα, γεγονός που αυξάνει το κόστος σε χώρο, χρόνο, χρήμα.

[9] Πολλοί συγγραφείς ορίζουν έτσι τους επαναληπτικούς κώδικες. Στα επόμενα και εμείς, όταν αναφερόμαστε σε επαναληπτικούς κώδικες, θα εννοούμε τους κώδικες $\mathcal{R}_p(k)$.

Παράδειγμα. Έστω ότι εκτελούμε το πείραμα της ρίψης ενός νομίσματος και συμφωνούμε να μεταδίδουμε τα αποτελέσματα των ρίψεων χρησιμοποιώντας τον κώδικα $\mathcal{C} = \{0, 1\}$. Αν το αποτέλεσμα είναι **γράμματα** αποστέλλουμε 0, αν το αποτέλεσμα είναι **κεφαλή** αποστέλλουμε 1. Προφανώς κάθε αλλοίωση του (μοναδικού) μεταδιδόμενου χαρακτήρα δίνει εσφαλμένο αποτέλεσμα κατά την αποκωδικοποίηση. (Ο κώδικας που χρησιμοποιούμε διορθώνει μηδέν το πλήθος λάθη, αφού έχει ελάχιστη απόσταση ένα). Αν τώρα συμφωνήσουμε να μεταδίδουμε τα αποτελέσματα των ρίψεων αποστέλλοντας 000 για το αποτέλεσμα **γράμματα** και 111 για το αποτέλεσμα **κεφαλή** χρησιμοποιώντας τον 3- επαναληπτικό κώδικα $\mathcal{C}_3 = \{000, 111\}$, τότε μπορούμε να ανιχνεύσουμε και να διορθώσουμε (μέχρι) ένα λάθος, αλλά δεν μπορούμε να ανιχνεύσουμε περισσότερα λάθη (βλέπε Θεώρημα 1.3.22).

Η $(\mathbf{u}, \mathbf{u}+\mathbf{v})$- κατασκευή

Θα τελειώσουμε την παράγραφο αναφέροντας έναν τρόπο κατασκευής ενός κώδικα από δύο άλλους κώδικες, είναι μια μέθοδος που εφαρμόζεται στην κατασκευή της οικογένειας των Reed-Muller κωδίκων (ιδέ στη σελίδα 149).

Έστω $\mathcal{C}_1, \mathcal{C}_2$ δύο κώδικες επί του ιδίου αλφαβήτου, το οποίο είναι ένα πεπερασμένο σώμα, με παραμέτρους (n, M_1, d_1) και (n, M_2, d_2) αντίστοιχα. Για $\mathbf{c} \in \mathcal{C}_1$ και $\mathbf{d} \in \mathcal{C}_2$ λαμβάνουμε το άθροισμα $\mathbf{c}+\mathbf{d}$ (το άθροισμα ορίζεται κατά συντεταγμένες, καθότι οι δύο κώδικες είναι ισομήκεις και ορίσθηκαν επί του ιδίου αλφαβήτου, το οποίο είναι σώμα). Κατόπιν από την παράθεση των λέξεων $\mathbf{c}$ και $\mathbf{c}+\mathbf{d}$ προκύπει η λέξη $\mathbf{c}(\mathbf{c}+\mathbf{d})$. Εφαρμόζουμε τη διαδικασία αυτή για όλα τα στοιχεία των $\mathcal{C}_1$ και $\mathcal{C}_2$. Το σύνολο $\mathcal{C}_1 \oplus \mathcal{C}_2 = \{\mathbf{c}(\mathbf{c}+\mathbf{d}) \mid \mathbf{c} \in \mathcal{C}_1, \mathbf{d} \in \mathcal{C}_2\}$ είναι ένας $(2n, M_1 \cdot M_2, \bar{d})$ κώδικας.
Ας υπολογίσουμε την ελάχιστη απόσταση $\bar{d}$. Έστω δύο (κωδικο)λέξεις $\mathbf{v}_1 = \mathbf{c}_1(\mathbf{c}_1+\mathbf{d}_1)$ και $\mathbf{v}_2 = \mathbf{c}_2(\mathbf{c}_2+\mathbf{d}_2)$. Διακρίνουμε περιπτώσεις, αν $\mathbf{d}_1 = \mathbf{d}_2$, τότε $d(\mathbf{v}_1, \mathbf{v}_2) = 2d(\mathbf{c}_1, \mathbf{c}_2) \geq 2d_1$. (Υπάρχουν (κωδικο)λέξεις $\mathbf{c}_1, \mathbf{c}_2 \in \mathcal{C}_1$ που η προηγούμενη ανισότητα γίνεται ισότητα). Στην περίπτωση, όπου $\mathbf{d}_1 \neq \mathbf{d}_2$ έχουμε από την Πρόταση 1.2.10 $d(\mathbf{v}_1, \mathbf{v}_2) = w(\mathbf{v}_1 - \mathbf{v}_2) = w(\mathbf{c}_1 - \mathbf{c}_2) + w(\mathbf{c}_1 - \mathbf{c}_2 + \mathbf{d}_1 - \mathbf{d}_2) \geq w(\mathbf{d}_1 - \mathbf{d}_2) = d(\mathbf{d}_1, \mathbf{d}_2) \geq d_2$. Για $\mathbf{c}_1 = \mathbf{c}_2$ και $\mathbf{d}_1, \mathbf{d}_2 \in \mathcal{C}_2$ έτσι ώστε $d(\mathbf{d}_1, \mathbf{d}_2) = d_2$ οι προηγούμενες ανισότητες γίνονται ισότητες, οπότε έχουμε αποδείξει την εξής πρόταση.

Πρόταση 1.4.12. *Με τις προηγούμενες υποθέσεις έχουμε*
$d(\mathcal{C}_1 \oplus \mathcal{C}_2) = min\{2d_1, d_2\}$.

1.4.2 Μεγιστικοί κώδικες

Έστω, για παράδειγμα, ο δυαδικός κώδικας $\mathcal{C} = \{\,0000,\, 1111,\, 0011\,\}$ μήκους 4, μεγέθους 3 και ελάχιστης απόστασης 2. Ο κώδικας αυτός ανιχνεύει μηδέν λάθη (π. χ. Αν λάβουμε τη λέξη 0010, αυτή ισαπέχει από τις (κωδικο)λέξεις 0000 και 0011, άρα δεν διορθώνεται παρ'ολο που διαφέρει από αυτές μόνο κατά ένα χαρακτήρα). Αυτό δεν σημαίνει ότι δεν μπορεί να διορθώσει καμία λέξη (π. χ. Αν λάβουμε τη λέξη 1000, τότε αυτή κατά την αποκωδικοποίηση διορθώνεται και αποκωδικοποιείται ως η λέξη 0000). Αν στον προηγούμενο κώδικα επισυνάψουμε τη λέξη 1100, τότε ο επαυξημένος κώδικας $\bar{\mathcal{C}} = \{\,0000,\, 1111,\, 0011,\, 1100\,\}$ έχει το ίδιο μήκος και την ίδια ελάχιστη απόσταση με τον κώδικα $\mathcal{C}$, αλλά δεν διορθώνει καμία λέξη με ένα λάθος (γιατί;). Πολύ δε περισσότερο πολλές λέξεις που λαμβάνονται και εμπεριέχουν δύο λάθη συμπίπτουν με (κωδικο)λέξεις, οπότε αποκωδικοποιούνται λανθασμένα (π. χ. Αν έχει σταλεί η λέξη 0000 και λάβουμε τη λέξη 1100, τότε αυτή ανήκει στον κώδικα και επομένως θεωρείται, λανθασμένα, ότι εστάλει αυτή).

Επομένως αναρωτιέται κάποιος, προς τι αύξηση του δοθέντος κώδικα;
Πέραν του ότι ο νέος κώδικας είναι *πλουσιώτερος* σε λέξεις, μπορούμε να διαχειρισθούμε αποτελεσματικότερα την πιθανότητα λανθασμένης αποκωδικοποίησης.

Ορισμός 1.4.13. *Ένας $r-$αδικός $(n,\, M,\, d)$ κώδικας $\mathcal{C}$ θα λέγεται μεγιστικός αν δεν υπάρχει $r-$αδικός $(n,\, M+1,\, d)$ κώδικας $\bar{\mathcal{C}}$ έτσι ώστε $\mathcal{C} \subseteq \bar{\mathcal{C}}$*

Προφανώς κάθε κώδικας περιέχεται σε (τουλάχιστον) ένα μεγιστικό κώδικα.

Επίσης ένας $(n,\, M,\, d)$ κώδικας $\mathcal{C}$ είναι μεγιστικός αν και μόνο αν για κάθε λέξη $\mathbf{x} \in \mathbb{A}^n$ υπάρχει μια (κωδικο)λέξη $\mathbf{c} \in \mathcal{C}$ τέτοια ώστε $d(\mathbf{x},\, \mathbf{c}) < d$ (γιατί;).

Έστω $\mathcal{C}$ ένας μεγιστικός κώδικας, υποθέτουμε ότι εστάλει η (κωδικο)λέξη $\mathbf{c}$ και ελήφθει λέξη $\mathbf{x}$ στην οποία έχουν υπεισέλθει τουλάχιστον d το πλήθος λάθη (δηλαδή το διάνυσμα λάθους $\mathbf{x} - \mathbf{c}$ έχει βάρος τουλάχιστον d και επομένως $d(\mathbf{x},\, \mathbf{c}) \geq d$). Επειδή ο κώδικας είναι μεγιστικός, υπάρχει σίγουρα μια (κωδικο)λέξη η οποία είναι πλησιέστερη στη $\mathbf{x}$ απ'οτι η $\mathbf{c}$. Επομένως αν κατά την αποκωδικοποίηση εφαρμόσουμε την αρχή της πλησιέστερης λέξης, τότε οποσδήποτε θα έχουμε λανθασμένη αποκωδικοποίηση.

Έστω ότι έχουμε έναν δυαδικό συμμετρικό δίαυλο επικοινωνίας, όπου η πιθανότητα μετάδοσης λάθους χαρακτήρα είναι ίση με p, δηλαδή
$p(\textit{ελήφθει ο χαρακτήρας } 1 \mid \textit{εστάλει ο χαρακτήρας } 0) =$
$= p(\textit{ελήφθει ο χαρακτήρας } 0 \mid \textit{εστάλει ο χαρακτήρας } 1) = p.$
Η πιθανότητα να μεταδοθούν k το πλήθος λανθασμένοι χαρακτήρες είναι ίση με $\binom{n}{k} p^k (1-p)^{n-k}$. Επομένως για την πιθανότητα λανθασμένης αποκωδικοποίησης μιας λέξης έχουμε

$$p(\textit{λανθασμένης αποκωδικοποίησης}) \geq \sum_{k=d}^{n} \binom{n}{k} p^k (1-p)^{n-k}.$$

Από την άλλη πλευρά όμως, σε οποιονδήποτε κώδικα με ελάχιστη απόσταση ίση με d, το πλήθος των λαθών που μπορούν να διορθωθούν είναι ίσον με $\left[\frac{d-1}{2}\right]$, συνεπώς για την πιθανότητα σωστής αποκωδικοποίσης έχουμε

$$p(\textit{σωστής αποκωδικοποίησης}) \geq \sum_{k=0}^{\left[\frac{d-1}{2}\right]} \binom{n}{k} p^k (1-p)^{n-k}.$$

Δηλαδή

$$p(\textit{λανθασμένης αποκωδικοποίησης}) =$$

$$= 1 - p(\textit{σωστής αποκωδικοποίησης}) \leq 1 - \sum_{k=0}^{\left[\frac{d-1}{2}\right]} \binom{n}{k} p^k (1-p)^{n-k}.$$

Άρα τελικά

$$\sum_{k=d}^{n} \binom{n}{k} p^k (1-p)^{n-k} \leq p(\textit{λανθασμένης αποκωδικοποίησης}) \leq 1 - \sum_{k=0}^{\left[\frac{d-1}{2}\right]} \binom{n}{k} p^k (1-p)^{n-k}.$$

Όπως βλέπουμε ένας μεγιστικός κώδικας υπερτερεί έναντι των κωδίκων που περιέχει ως (υπο)κώδικες (πλουσιώτερο λεξιλόγιο), αλλά υστερεί στο γεγονός ότι έχει αυξημένη πιθανότητα λανθασμένης αποκωδικοποίησης (λέξεις που περιέχουν τουλάχιστον d το πλήθος λάθη αποκωδικοποιούνται οποσδήποτε λανθασμένα).

1.4.3 Ασκήσεις

1. Έστω $\mathcal{E}_n$ ο δυαδικός κώδικας που αποτελείται από όλες τις λέξεις μήκους n με άρτιο βάρος. Έστω ο κώδικας $\mathcal{D} = \mathbb{Z}_2^{n-1}$. Δείξτε ότι ο $\mathcal{E}_n$ προέρχεται από τον $\mathcal{D}$ με την επισύναψη ενός ψηφίου ελέγχου ισοτιμίας. Ποιές είναι οι παράμετροι του κώδικα $\mathcal{E}_n$;

2. Κατασκευάστε έναν δυαδικό κώδικα με παραμέτρους (7, 6, 2) και κατόπιν εφαρμόζοντας μια σμίκρυνση και μια σύμπτυξη να προέλθει ένας (6, 4, 3) κώδικας.

3. Έστω $\mathcal{C}$ ένας κώδικας με παραμέτρους $(n,\, M,\, d)$. Δείξτε ότι μπορούμε να κατασκευάσουμε έναν άλλο κώδικα $\mathcal{D}$ με παραμέτρους $(n+1,\, M+2,\, 1)$, έτσι ώστε ο κώδικας $\mathcal{C}$ να προέρχεται από τον $\mathcal{D}$ εφαρμόζοντας διαδοχικά μια σμίκρυνση και μια σύμπτυξη.

4. Έστω $\mathcal{C}$ ένας δυαδικός κώδικας του οποίου όλα τα στοιχεία έχουν άρτιο βάρος. Δείξτε ότι η απόσταση δύο οποιωνδήποτε (κωδικο)λέξεων είναι άρτια. Τί συμπεραίνετε για την ελάχιστη απόσταση ένος κώδικα που προέρχεται από έναν δυαδικό κώδικα με την επισύναψη ένος ψηφίου ελέγχου ισοτιμίας;

5. Δείξτε ότι αν υπάρχει ένας δυαδικός $(n,\, M,\, d)$ κώδικας με d άρτιο, τότε υπάρχει ένας δυαδικός $(n,\, M,\, d)$ κώδικας, του οποίου όλες οι (κωδικο)λέξεις έχουν άρτιο βάρος.

6. Έστω $\mathcal{C}$ ένας δυαδικός κώδικας.

   i) Στον κώδικα $\mathcal{C}$ εφαρμόζουμε διαδοχικά δύο φορές την διαδικασία της επισύναψης ενός ψηφίου ελέγχου ισοτιμίας. Τι κώδικας θα προκύψει; Έχει νόημα η δεύτερη επισύναψη ψηφίου ελέγχου ισοτιμίας;

   ii) Στον κώδικα $\mathcal{C}$ επισυνάπτουμε ένα ψηφίο ελέγχου ισοτιμίας και κατόπιν στο τέλος κάθε στοιχείου έναν χαρακτήρα έτσι ώστε το βάρος κάθε λέξης που προκύπτει να είναι περιττό. Να συγκρίνετε την ελάχιστη απόσταση του αρχικού κώδικα $\mathcal{C}$ με την ελάχιστη απόσταση του κώδικα $\mathcal{D}$ που προκύπτει από την παραπάνω διαδικασία.
   Αν στον αρχικό κώδικα $\mathcal{C}$ εφαρμόσουμε αντίστροφη διαδικασία, δηλαδή πρώτα στο τέλος κάθε στοιχείου επισυνάψουμε έναν χαρακτήρα έστι ώστε το βάρος κάθε λέξης που προκύπτει να είναι περιττό και κατόπιν επισυνάψουμε ένα ψηφίο ελάγχου ισοτιμίας, ο κώδικας $\mathcal{E}$ που προκύπτει τι σχέση έχει με τους προηγούμενους κώδικας $\mathcal{C}$ και $\mathcal{D}$;

7. Πόσοι μη ισοδύναμοι δυαδικοί κώδικας μήκους n με δύο μόνο στοιχεία υπάρχουν;

8. Εφαρμόζοντας την $(\mathbf{u},\, \mathbf{u}+\mathbf{v})$- κατασκευή να κατασκευάσετε τον κώδικα $\mathcal{C}_1 \oplus \mathcal{C}_2$ στις ακόλουθες περιπτώσεις:
   i) $\mathcal{C}_1 = \{\, 000,\, 001,\, 111 \,\},\ \mathcal{C}_2 = \{\, 100,\, 011,\, 001 \,\}$
   ii) Ο $\mathcal{C}_1$ είναι ο δυαδικός $(4,\, 8,\, 2)$ κώδικας που αποτελείται από τις οκτώ (κωδικο)λέξεις μήκους 4 και είναι αρτίου βάρους και ο $\mathcal{C}_2$ είναι ο επαναληπτικός κώδικας $\mathcal{R}_2(4)$.

   Στις παραπάνω περιπτώσεις να υπολογίσετε τις παραμέτρους του κώδικα $\mathcal{C}_1 \oplus \mathcal{C}_2$.

9. Έστω $\mathcal{C}$ ένας $p-$αδικός κώδικας και $\overline{\mathcal{C}}$ ο κώδικας που προκύπτει από τον $\mathcal{C}$ επισυνάπτοντας ένα ψηφίο ελέγχου ισοτιμίας. Τι σχέση έχουν οι ελάχιστες αποστάσεις των κωδίκων $\mathcal{C}$ $p-$αδικός και $\overline{\mathcal{C}}$;
Προσπαθήστε με έναν τριαδικό κώδικα.

10. Έστω $\mathcal{C}$ ένας κώδικας, ο οποίος δεν είναι μεγιστικός. Πώς μπορούμε να επισυνάψουμε στοιχεία στον $\mathcal{C}$ έως ότου να επιτύχουμε έναν μεγιστικό κώδικα;

1.5 Τέλειοι κώδικες

Στην αρχή ορίζοντας την απόσταση Hamming είχαμε παρατηρήσει (Παρατήρηση 1.2.4) ότι μπορούμε να κάνουμε *Γεωμετρία* στο σύνολο $\mathbb{A}^n$, όπου $\mathbb{A}$ είναι ένα αλφάβητο (συνήθως το $\mathbb{Z}_p$ ή γενικότερα ένα πεπερασμένο σώμα). Εδώ θα δούμε μια *Γεωμετρική* θεώρηση των κωδίκων ως πρός την ικανότητά τους να διορθώνουν λάθη.
Αυτό θα μας οδηγήσει σε μια σημαντική κατηγορία κωδίκων, τους τέλειους κώδικες.

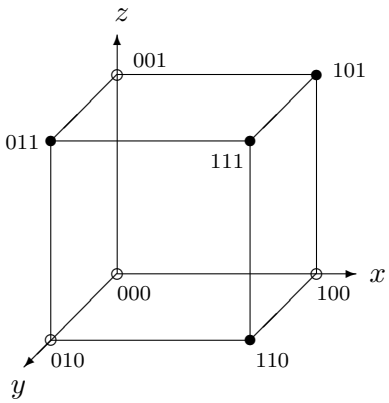
1.5.1 Σφαίρες ομαδοποίησης και τέλειοι κώδικες

Ορισμός 1.5.1. *Έστω ένα αλφάβητο $\mathbb{A}$ με q το πλήθος στοιχεία και n ένας φυσικός ακέραιος. Για κάθε $\mathbf{x} \in \mathbb{A}^n$ και κάθε πραγματικό μη αρνητικό αριθμό r ορίζουμε την* **σφαίρα** *(διάστασης n με κέντρο το στοιχείο $\mathbf{x}$ και ακτίνα ίση με r το σύνολο $S_q^n(\mathbf{x}, r) = \{\, \mathbf{y} \in \mathbb{A}^n \mid d(\mathbf{x}, \mathbf{y}) \leq r \,\}$* [10] *.*

Παραδείγματα 1.5.2. 1. Η σφαίρα $S_2^3(101, 2)$ στο $\mathbb{Z}_2^3$ αποτελείται από όλες τις δυαδικές λέξεις μήκους 3 οι οποίες απέχουν απόσταση τουλάχιστον 2 από την 101, και προφανώς $S_2^3(101, 2) = \{\, 101, 001, 111, 100, 011, 000, 110 \,\}$.

2. Στο επόμενο σχήμα παρίσταται γεωμετρικά η σφαίρα $S_2^3(111, 1)$ στο $\mathbb{Z}_2^3$, όπου τα στοιχεία που ανήκουν σ' αυτή είναι οι κορυφές του κύβου με την έντονη στίξη.

[10] Όταν δεν υπάρχει κίνδυνος σύγχυσης ως προς το q και το n αντί για $S_q^n(\mathbf{x}, r)$ θα γράφουμε $S(\mathbf{x}, r)$



Δυστυχώς είναι δύσκολο να κάνουμε σχεδιαστική αναπαράσταση μιας σφαίρας στην περίπτωση όπου η διάσταση είναι $n \geq 4$.

Άμεσα συνδεδεμένη με την έννοια της σφαίρας είναι η έννοια του **όγκου** της . Ο όγκος μιας σφαίρας $S_q^n(\mathbf{x},\, r)$ είναι ο αριθμός των λέξεων οι οποίες περιέχονται μέσα στη σφαίρα. Προφανώς (γιατί;) ο όγκος μιας σφαίρας δεν εξαρτάται από την επιλογή του κέντρου της $\mathbf{x}$, για το λόγο αυτό συνήθως συμβολίζεται $V_q(n,\, r)$. Μπορούμε να υπολογίσουμε εύκολα τον όγκο μιας σφαίρας. Έστω μια λέξη $\mathbf{x} \in \mathbb{A}^n$, για $0 \leq k \leq n$ ο αριθμός των λέξεων, οι οποίες διαφέρουν σε k θέσεις από την $\mathbf{x}$ (έχουν απόσταση ίση με k από την $\mathbf{x}$), είναι προφανώς ίσος με $\binom{n}{k}(q-1)^k$. Επομένως αθροίζοντας από 0 έως r έχουμε για τον όγκο της σφαίρας

$$V_q(n,\, r) \;=\; \sum_{k\,=\,0}^{r} \binom{n}{k} (q-1)^k \;.$$

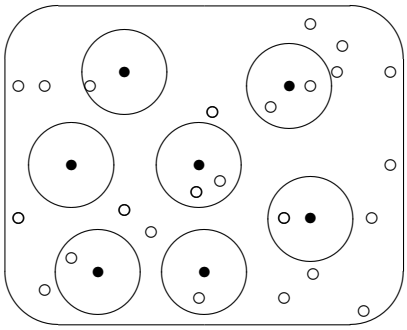
(Ο αριθμός r είναι πραγματικός αλλά στο προηγούμενο άθροισμα, όπου ο k είναι ακέραιος δεν υπάρχει σύγχυση καθότι το k λαμβάνει τιμές από 0 έως $[r]$.)

Αξίζει να σημειωθεί ότι στην περίπτωση όπου το αλφάβητο $\mathbb{A}$ είναι το $\mathbb{Z}_2$, τότε ο όγκος μιας σφαίρας ακτίνας r είναι το άθροισμα των r πρώτων διωνυμικών συντελεστών, δηλαδή

$$V_2(n,\, r) \;=\; \sum_{k\,=\,0}^{r} \binom{n}{k} \;.$$

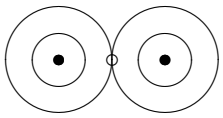
Έστω $\mathcal{C} \subseteq \mathbb{A}^n$ ένας $(n,\, M,\, d)$ κώδικας. Σκοπός μας είναι με κέντρο κάθε (κωδικο)λέξη να κατασκευάσουμε σφαίρες με όσο το δυνατόν μεγαλύτερη κοινή ακτίνα, αλλά να μην τέμνονται μεταξύ τους.

Στό επόμενο σχήμα οι • αναπαριστούν τις (κωδικο)λέξεις, ενώ οι ∘ αναπαριστούν τα υπόλοιπα στοιχεία του $\mathbb{A}^n$.

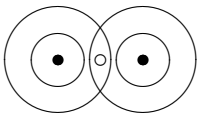


Υποθέτουμε ότι η ελάχιστη απόσταση του κώδικα είναι άρτια ίση με $d = 2\lambda + 2$ και $\mathbf{c}$, $\mathbf{d}$ είναι δύο (κωδικο)λέξεις που απέχουν μεταξύ τους απόσταση ίση με την ελάχιστη απόσταση του κώδικα. Τότε υπάρχει μια (τουλάχιστον) λέξη $\mathbf{x} \in \mathbb{A}^n$ η οποία ισαπέχει από τις $\mathbf{c}$ και $\mathbf{d}$ (γιατί;). Αν πάρουμε σφαίρες με κέντρα τις $\mathbf{c}$ και $\mathbf{d}$ και ακτίνα $\lambda + 1$, τότε οι δύο σφαίρες *εφάπτονται* στη λέξη $\mathbf{x}$. Αν όμως οι σφαίρες έχουν ακτίνα ίση με λ, τότε αυτές είναι ξένες μεταξύ τους.
Αν η ελάχιστη απόσταση του κώδικα είναι περιττή ίση με $d = 2\lambda + 1$ και $\mathbf{c}$, $\mathbf{d}$ είναι δύο (κωδικο)λέξεις που απέχουν μεταξύ τους απόσταση ίση με την ελάχιστη απόσταση του κώδικα. Τότε δεν υπάρχει λέξη $\mathbf{x} \in \mathbb{A}^n$ η οποία να ισαπέχει από τις $\mathbf{c}$ και $\mathbf{d}$ απόσταση ίση με λ (γιατί;). Αν πάρουμε σφαίρες με κέντρα τις $\mathbf{c}$ και $\mathbf{d}$ και ακτίνα $\lambda + 1$, τότε οι δύο σφαίρες *τέμνονται* σε μια (τουλάχιστον) λέξη (γιατί;). Αν όμως οι σφαίρες έχουν ακτίνα ίση με λ, τότε αυτές είναι ξένες μεταξύ τους.

Η προηγούμενη συζήτηση θα μπορούσε να αναπαρασταθεί στα επόμενα σχήματα.



$d = 2\lambda + 2$



$d = 2\lambda + 1$

Όπως βλέπουμε και στις δύο περιπτώσεις σφαίρες με κέντρα (κωδικο)λέξεις και ακτίνα ίση με $\lambda = \left[\frac{d-1}{2}\right]$ είναι ξένες μεταξύ τους και η ακτίνα αυτή είναι η μεγαλύτερη δυνατή με την ιδιότητα αυτή.

Ορισμός 1.5.3. *Έστω $\mathcal{C} \subseteq \mathbb{A}^n$ ένας (n, M, d) $q-$αδικός κώδικας. Ο μεγαλύτερος ακέραιος αριθμός r για τον οποίο οι σφαίρες $S_q^n(\mathbf{c}, r)$ με κέντρο οποιαδήποτε (κωδικο)λέξη $\mathbf{c}$ είναι ξένες μεταξύ τους, λέγεται* **ακτίνα ομαδοποίησης** *και συμβολίζεται με $pr(\mathcal{C})$. Οι δε αντίστοιχες σφαίρες $S_q^n(\mathbf{c}, r)$ ονομάζονται σφαίρες* **ομαδοποίησης** .

Πρόταση 1.5.4. *Σε έναν (n, M, d) κώδικα $\mathcal{C} \subseteq \mathbb{A}^n$ η ακτίνα ομαδοποίησης είναι ίση με $pr(\mathcal{C}) = \left[\frac{d-1}{2}\right]$.*

Απόδειξη. Η απόδειξη έχει προηγηθεί.

□

Θεώρημα 1.5.5. *Ένας κώδικας $\mathcal{C}$ διορθώνει λ λάθη αν και μόνο αν για κάθε (κωδικο)λέξη $\mathbf{c}$ οι σφαίρες $S_q^n(\mathbf{c}, \lambda)$ είναι ξένες.*

Απόδειξη. Υποθέτουμε ότι ο κώδικας διορθώνει λ λάθη και ότι υπάρχουν δύο (κωδικο)λέξεις $\mathbf{c}$ και $\mathbf{d}$ για τις οποίες υπάρχει λέξη $\mathbf{x} \in S_q^n(\mathbf{c}, \lambda) \cap S_q^n(\mathbf{d}, \lambda)$. Επομένως έχουμε ότι $d(\mathbf{c}, \mathbf{d}) \leq d(\mathbf{c}, \mathbf{x}) + d(\mathbf{x}, \mathbf{d}) \leq \lambda + \lambda = 2\lambda$. Αλλά από το Θεώρημα 1.3.16 έχουμε ότι $d(\mathcal{C}) \geq 2\lambda + 1$, άτοπο.

Το αντίστροφο είναι προφανές.

□

Πόρισμα 1.5.6. *Ένας κώδικας διορθώνει ακριβώς λ λάθη αν και μόνο αν η ακτίνα ομαδοποίησης είναι ιση με λ.*

Παρατηρήσεις 1.5.7.

1. Από τα προηγούμενα βλέπουμε *γεωμετρικά* ότι για κάθε κωδικολέξη η αντίστοιχη σφαίρα ομαδοποίησης έχει *αιχμαλωτίσει* όλες τις λέξεις, οι οποίες σύμφωνα με την αρχή της αποκωδικοποίησης ως προς την πλησιέστερη λέξη *έλκονται* από το κέντρο της σφαίρας και *ταυτίζονται* μ΄ αυτό.

2. Λαμβάνοντας την (διακεκριμένη) ένωση των σφαιρών ομαδοποίησης για κάθε (κωδικο)λέξη έχουμε $\bigcup_{i=1}^{M} S_q^n(\mathbf{c}_i, \lambda) \subseteq \mathbb{A}^n$.

Θεώρημα 1.5.8. ***Το φράγμα ομαδοποίησης σφαιρών ή φράγμα Hamming***
Έστω $\mathcal{C}$ ένας (n, M, d) κώδικας επί του αλφάβητου $\mathbb{A}$ με $\mid \mathbb{A} \mid = q$, τότε ισχύει $M \leq q^n/V$, όπου $V = V_q(n, r) = \sum_{k=0}^{r} \binom{n}{k}(q-1)^k$ και $r = pr(\mathcal{C}) = \left[\frac{d-1}{2}\right]$ είναι η ακτίνα ομαδοποίησης.

Απόδειξη. Η απόδειξη απορρέει από τα προηγούμενα, εδώ απλώς την επαναλαμβάνουμε.

Αν για κάθε (κωδικο)λέξη πάρουμε την αντίστοιχη σφαίρα ομαδοποίησης έχουμε M το πλήθος ξένες σφαίρες όλες με την ίδια ακτίνα ομαδοποίησης

$r = pr(\mathcal{C}) = \left[\frac{d-1}{2}\right]$. Το πλήθος των λέξεων που περιέχονται σε κάθε σφαίρα δεν εξαρτάται από το κέντρο της, αλλά μόνο από την (κοινή) ακτίνα και για όλες είναι ίσο με τον όγκο μιας απ' αυτές, ο οποίος έχουμε δείξει ότι είναι ίσος με $V = V_q(n, r) = \sum_{k=0}^{r} \binom{n}{k}(q-1)^k$. Επομένως το πλήθος των λέξεων που περιέχεται σε όλες τις σφαίρες ομαδοποίησης είναι ίσο με $M \cdot V$, που φυσικά δεν υπερβαίνει το συνολικό πλήθος των λέξεων μήκους n με χαρακτήρες από το αλφάβητο $\mathbb{A}$ με τα q το πλήθος στοιχεία.

□

Ορισμός 1.5.9. *Έστω $\mathcal{C} \subseteq \mathbb{A}^n$ ένας (n, M, d) κώδικας. Ο μικρότερος ακέραιος αριθμός r για τον οποίο οι σφαίρες $S_q^n(\mathbf{c}, r)$ με κέντρο οποιαδήποτε (κωδικο)λέξη* **c καλύπτουν** *το σύνολο $\mathbb{A}^n$ λέγεται* **ακτίνα κάλυψης** *και συμβολίζεται με $cr(\mathcal{C})$. Οι δε αντίστοιχες σφαίρες $S_q^n(\mathbf{c}, r)$ ονομάζονται σφαίρες* **κάλυψης** .

Προφανώς οι σφαίρες κάλυψης δεν είναι κατ' ανάγκη ξένες μεταξύ τους. Από την άλλη πλευρά έχουμε δεί ότι οι σφαίρες ομαδοποίησης είναι μεν ξένες μεταξύ τους, αλλά δεν καλύπτουν κατ΄ ανάγκη ολόκληρο το $\mathbb{A}^n$. Επομένως γεννάται το ερώτημα:
Υπάρχει περίπτωση να μπορούμε να καλύψουμε το $\mathbb{A}^n$ με ξένες σφαίρες; Με άλλα λόγια, υπάρχει περίπτωση οι σφαίρες κάλυψης να συμπίπτουν με τις σφαίρες ομαδοποίησης;

Ορισμός 1.5.10. *Ένας (n, M, d) κώδικας $\mathcal{C} \subseteq \mathbb{A}^n$ ονομάζεται* **τέλειος** *αν η ακτίνα ομαδοποίησης είναι ίση με την ακτίνα κάλυψης ($pr(\mathcal{C}) = cr(\mathcal{C})$).*

Παράδειγμα 1.5.11. Ο επαναληπτικός δυαδικός κώδικας $\mathcal{C} = \{000, 111\}$ είναι προφανώς τέλειος.

Μια άμεση συνέπεια του ορισμού είναι η εξής πρόταση.

Πρόταση 1.5.12. *Ένας (n, M, d) κώδικας $\mathcal{C} \subseteq \mathbb{A}^n$ με $|\,\mathbb{A}\,| = q$ είναι τέλειος αν και μόνο αν η ελάχιστη απόσταση είναι περιττή $d = 2r + 1$ και ισχύει*

$$M = \frac{q^n}{\sum_{k=0}^{r} \binom{n}{k}(q-1)^k}. \tag{1.5.2}$$

Απόδειξη. Το ότι ένας τέλειος κώδικας αναγκαστικά έχει περιττή ελάχιστη απόσταση έπεται από τον ορισμό και την συζήτηση που προηγήθηκε του Ορισμού 1.5.3. Τα υπόλοιπα έπονται άμεσα από τον ορισμό και το Θεώρημα 1.5.8.

□

Όπως βλέπουμε από τον ορισμό ένας τέλειος κώδικας με παραμέτρους (n, M, d) έχει την ιδιότητα να αποκωδικοποιεί κάθε λέξη $\mathbf{x} \in \mathbb{A}^n$. Μάλιστα δε αν έχουν

υπεισέλθει μέχρι $\left[\frac{d-1}{2}\right]$ το πλήθος λάθη, τότε, σύμφωνα με την αρχή αποκωδικοποίησης ως προς τη πλησιέστερη λέξη, η αποκωδικοποιήση είναι σωστή.

Το πρόβλημα της ανακάλυψης όλων των τέλειων κωδίκων παραμένει ανοικτό. Η σημαντικότερη πρόοδος έχει γίνει στην περίπτωση όπου το μέγεθος του κώδικα ισούται με τη δύναμη ενός πρώτου αριθμού. Επ' αυτού θα επανέλθουμε αργότερα.

Προς το παρόν θα περιορισθούμε σε μια απλή προσέγγιση του προβλήματος αναζητώντας θετικούς ακεραίους q, n, M και $d = 2r+1$ που ικανοποιούν τη σχέση 1.5.2. Πριν προχωρήσουμε πρέπει να τονίσουμε ότι η υπάρξη τέτοιων αριθμών **δεν** συνεπάγεται την ύπαρξη κωδίκων με αυτές τις παραμέτρους, όπως θα δούμε αργότερα.

Είναι εύκολο (και αφίνεται ως άσκηση) να επαληθεύσουμε ότι κώδικες (αν υπάρχουν) με τις παρακάτω οικογένειες παραμέτρων είναι τέλειοι.

1. $(n,\, M,\, d) = (n,\, q^n,\, 1)$
2. $(n,\, M,\, d) = (n,\, 1,\, ?)$
3. $(n,\, M,\, d) = (2r+1,\, 2,\, 2r+1)$
4. $(n,\, M,\, d) = (\frac{q^r-1}{q-1},\, q^{n-r},\, 3),\ r \geq 2$
5. $(n,\, M,\, d) = (23,\, 2^{11},\, 7)$
6. $(n,\, M,\, d) = (90,\, 2^{78},\, 5)$
7. $(n,\, M,\, d) = (11,\, 3^6,\, 5)$

Οι κώδικες που ανήκουν στην πρώτη και δεύτερη οικογένεια αποτελούν ακραίες περιπτώσεις, όπου στην μεν πρώτη περίπτωση ο κώδικας αποτελείται από όλες τις λέξεις μήκους n και δεν διορθώνει κανένα λάθος, στην δε δεύτερη περίπτωση ο κώδικας αποτελείται από μία μόνο λέξη (μάλιστα δε δεν ορίζεται κάν η ελάχιστη απόσταση). Στην τρίτη περίπτωση ανήκουν οι δυαδικοί επαναληπτικοί κώδικες περιττού μήκους οι οποίοι αποτελούνται από δύο μόνο λέξεις. Η τέταρτη οικογένεια περιλαμβάνει μια σημαντική κατηγορία κωδίκων, γνωστούς ως κώδικες Hamming, στους οποίους θα αναφερθούμε διεξοδικότερα στην Παράγραφο 3.1. Οι περιπτώσεις πέντε και επτά αντιστοιχούν στους περίφημους Golay κώδικες, στους οποίους επίσης θα αναφερθούμε αργότερα στην Παράγραφο 3.2. Τέλος έχει αποδειχθεί (βλέπε Θεώρημα 3.3.1 και Πρόταση 3.3.3) ότι δεν υπάρχουν κώδικες με παραμέτρους που να αντιστοιχούν στην έκτη περίπτωση.

Οι κώδικες που ανήκουν στις τρεις πρώτες οικογένειες αναφέρονται ως **τετριμμένοι** τέλειοι κώδικες. Όπως θα δούμε στην Παράγραφο 3.3 (αλλά δεν θα αποδείξουμε) οι μέχρι σήμερα γνωστοί τέλειοι κώδικες, στην ουσία [11] ανήκουν

[11] Επισημαίνουμε ότι αν βρούμε έναν κώδικα με κάποιες παραμέτρους, αυτό δεν σημαίνει ότι δεν υπάρχουν και άλλοι κώδικες με τις ίδιες παραμέτρους (βλέπε για παράδειγμα τους ισοδύναμους κώδικες)

σε μια από τις παραπάνω οικογένειες.

1.5.2 Φράγματα κωδίκων

Προηγουμένως ασχοληθήκαμε με τους μεγιστικούς κώδικες και είδαμε σε τι υπερέχουν και σε τι υστερούν. Εδώ ενδιαφερόμαστε για κώδικες οι οποίοι περιέχουν όσο το δυνατόν περισότερες (κωδικο)λέξεις, με δεδομένη την ελάχιστη απόσταση d και το μήκος n.

Ορισμός 1.5.13. *Έστω ένα αλφάβητο* $\mathbb{A}$ *με* r *το πλήθος στοιχεία,* n *και* d *φυσικοί αριθμοί και* $A_r(n,\, d) = \max\{\, M \mid$ *υπάρχει* $(n,\, M,\, d)$ *κώδικας*$\}$. *Ένας κώδικας* $\mathcal{C}$ *με μέγεθος ίσο με* $A_r(n,\, d)$ *θα λέγεται* **βέλτιστος** .

Προφανώς ένας βέλτιστος κώδικας είναι μεγιστικός, το αντίστροφο προφανώς (γιατί;) δεν ισχύει.

Ο προσδιορισμός των αριθμών $A_r(n,\, d)$ για τις διάφορες τιμές των παραμέτρων r, n και d έχει αναχθεί σε κεντρικό πρόβλημα στην Θεωρία Κωδίκων. Για μικρές τιμές των ανωτέρω παραμέτρων έχουν προσδιορισθεί (επακριβώς) οι αντίστοιχες τιμές $A_r(n,\, d)$, ο επόμενος πίνακας περιλαμβάνει μερικές τιμές για δυαδικούς κώδικες.

Μερικές τιμές του $A_2(n,\, d)$

n	$d = 3$	$d = 5$	$d = 7$
5	4	2	–
6	8	2	–
7	16	2	2
8	20	4	2
9	40	6	2
10	$72 - 79$	12	2
11	$144 - 158$	24	4
12	256	32	4
13	512	64	8
14	1024	128	16
15	2048	256	32
16	$2560 - 3276$	$256 - 340$	$36 - 37$

Γενικά όμως η προσπάθειες έχουν επικεντρωθεί στην εύρεση καλών (άνω και κάτω) φραγμάτων. Επίσης έχει μελετηθεί η ασυμπτωτική συμπεριφορά των τιμών $A_r(n,\, d)$ ως προς το λόγο $\delta = \frac{d}{n}$ καθώς το $n \longrightarrow \infty$.

Προφανώς στις ακραίες (και προφανείς) περιπτώσεις έχουμε:

$A_r(n,\, d) \leq r^n$
$A_r(n,\, 1) = r^n.$
$A_r(n,\, n) = r.$

Θεώρημα 1.5.14. *Για δυαδικούς κώδικες ισχύει*
$A_2(n,\, 2\lambda + 1) = A_2(n+1,\, 2\lambda + 2).$

Απόδειξη. Η απόδειξη έπεται άμεσα από το Θεώρημα 1.4.9 .

□

Παρατήρηση 1.5.15. Όπως θα έχετε παρατηρήσει ο προηγούμενος πίνακας αναφέρεται σε βέλτιστους κώδικες με περιττή ελάχιστη απόσταση. Από το προηγούμενο Θεώρημα βλέπουμε ότι είναι αρκετό να υπολογίσουμε τις τιμές $A_2(n,\, d)$ μόνο για περιττές (ή μόνο για άρτιες) τιμές του d.

Θεώρημα 1.5.16. $A_r(n,\, d) \leq r \cdot A_r(n-1,\, d)$.

Απόδειξη. Έστω $\mathcal{C}$ ένας βέλτιστος $r-$αδικός $(n,\, M,\, d)$ κώδικας (δηλαδή $M = A_r(n,\, d)$). Διαμερίζουμε το σύνολο των (κωδικο)λέξεων σε υποκώδικες έτσι ώστε κάθε υποκώδικας να περιέχει σε μια συγκεκριμένη συντεταγμένη (π. χ. στην τελευταία) τον ίδιο χαρακτήρα. Επομένως έχουμε το πολύ r το πλήθος τέτοιους υποκώδικες. Τουλάχιστον ένας απ' αυτούς τους υποκώδικες περιέχει τουλάχιστον M/r το πλήθος στοιχεία (γιατί;). Από έναν τέτοιο υποκώδικα διαγράφουμε τον κοινό χαρακτήρα από τη συγκεκριμένη θέση, οπότε προκύπτει ένας κώδικας μήκους $n-1$ και με ελάχιστη απόσταση τουλάχιστον ίση με d. Τελικά βλέπουμε ότι βέλτιστοι κώδικες μήκους $n-1$ περιέχουν τουλάχιστον M/r το πλήθος στοιχεία και το αποτέλεσμα έπεται.

□

Η διαδικασία που ακολουθήσαμε στο προηγούμενο θεώρημα αποτελεί συμπύκνωση του αρχικού κώδικα, βλέπε παρατηρήσεις 1.4.10 , σελ. 38.

Θεώρημα 1.5.17. (Φράγμα επικάλυψης σφαιρών ή κάτω φράγμα των Gilbert-Varshamov).

Για το μέγεθος ενός βέλτιστου κώδικα ισχύει $A_r(n,\, d) \geq r^n / V_r(n,\, d-1)$.

Απόδειξη. Έστω ένας $(n,\, M,\, d)$ βέλτιστος κώδικας $\mathcal{C}$ επί του αλφαβήτου $\mathbb{A}$ με $|\, \mathbb{A}\, | = r$ και $\mathbf{y} \in \mathbb{A}^n \backslash \mathcal{C}$. Τότε υπάρχει (κωδικο)λέξη $\mathbf{a} \in \mathcal{C}$ έτσι ώστε η $\mathbf{y}$ να ανήκει στη σφαίρα $S_r^n(\mathbf{a},\, d-1)$. Πράγματι αν η $\mathbf{y}$ δεν ανήκε σε καμία σφαίρα με κέντρο μια (κωδικο)λέξη και ακτίνα ίση με $d-1$, τότε θα είχαμε $d(\mathbf{x},\, \mathbf{y}) \geq d$ για κάθε $\mathbf{x} \in \mathcal{C}$. Επομένως ο κώδικας $\mathcal{C} \cup \{\, y \,\}$ θα είχε ελάχιστη απόσταση ίση με d και μέγεθος $M+1$, άτοπο διότι ο $\mathcal{C}$ είναι βέλτιστος. Επομένως έχουμε αποδείξει ότι οι σφαίρες με κέντρα τα στοιχεία του $\mathcal{C}$ και ακτίνα ίση με $d-1$ καλύπτουν το $\mathbb{A}^n$. Άρα $|\, \mathbb{A}\, |^n, = r^n \leq M \cdot V_r(n,\, d-1)$. Οπότε έπεται το αποτέλεσμα. □

Επειδή

$$V_r(n,\, d-1) \;=\; \sum_{k=0}^{d-1} \binom{n}{k} (r-1)^k$$

τη σχέση στο προηγούμενο Θεώρημα την συναντάμε και ως

$$A_r(n,\, d) \geq r^n / \sum_{k=0}^{d-1} \binom{n}{k} (r-1)^k \ .$$

Συνδυάζοντας το Θεώρημα 1.5.8 με το προηγούμενο Θεώρημα έχουμε:

Θεώρημα 1.5.18. $r^n/V_r(n,\, d-1) \leq A_r(n,\, d) \leq r^n/V_r(n,\, \left[\frac{d-1}{2}\right])$.

Πόρισμα 1.5.19. *Ένας τέλειος κώδικας είναι βέλτιστος.*

Απόδειξη. Η απόδειξη είναι άμεση, δεδομένου ότι η δεύτερη ανισότητα στο προηγούμενο θεώρημα είναι ισότητα στην περίπτωση ενός τέλειου κώδικα.

□

Τα παραπάνω (άνω και κάτω) φράγματα για το μέγεθος βέλτιστων κωδίκων δεν είναι τα καλλίτερα δυνατά.

Όπως θα δούμε στην περίπτωση των Γραμμικών Κωδίκων (βλέπε Πρόταση 2.2.30) μπορούμε να βελτιώσουμε το παραπάνω κάτω φράγμα.

Εδώ θα περιορισθούμε αναφέροντας μόνο δύο άλλα άνω φράγματα.

Θεώρημα 1.5.20. (Φράγμα Singleton)
Για βέλτιστους $r-$αδικούς κώδικες ισχύει $A_r(n,\, d) \leq r^{n-d+1}$.

Απόδειξη. Έστω $\mathcal{C}$ ένας $r-$αδικός $(n,\, M,\, d)$ κώδικας. Συμπτίσουμε τον κώδικα διαγράφοντας τις τελευταίες $d-1$ συντεταγμένες από όλες τις (κωδικο)λέξεις (ή γενικότερα τις ίδιες $d-1$ συντεταγμένες από κάθε (κωδικο)λέξη). Οι M το πλήθος λέξεις που προκύπτουν είναι διαφορετικές μεταξύ τους. Πράγματι, αν δύο από αυτές συνέπιπταν, τότε οι αρχικές λέξεις από τις οποίες προέρχονται θα διέφεραν στα διαγραφέντα τμήματα μήκους $d-1$, δηλαδή η μεταξύ τους απόσταση θα ήταν το πολύ ίση με $d-1$, άτοπο (γιατί;). Δηλαδή έχουμε κατασκευάσει ένα κώδικα μεγέθους M και μήκους $n-d+1$. Επομένως $M \leq r^{n-d+1}$.

□

Παρατηρήσεις 1.5.21.

1. Αν συγκρίνουμε το φράγμα Hamming και το φράγμα Singleton βλέπουμε ότι στην μεν πρώτη περίπτωση έχουμε $A_r(4,\, 3) \leq \frac{r^4}{4r-3}$, ενώ στη δεύτερη έχουμε $A_r(n,\, d) \leq r^{n-d+1}$. Οπότε για $r \geq 4$ το φράγμα Singleton είναι πολύ καλλίτερο.

2. Υπάρχουν περιπτώσεις, όπου το φράγμα Singleton είναι το καλλίτερο δυνατόν. Πράγματι, ο κώδικας
   $\mathcal{C} = \{\, aaa, abc, acd, adb, bca, cda, dba, cab, dac, bad, bdc, cbd, dcb, bbb, ccc, ddd \,\}$ είναι ένας $(3, 16, 2)$ κώδικας επί του αλφάβητου
   $\mathbb{A} = \{\, a, b, c, d \,\}$, επομένως για έναν βέλτιστο κώδικα με τις ίδιες παραμέτρους πρέπει να έχουμε $A_4(3, 2) \geq 16$. Αλλά σύμφωνα με το φράγμα Singleton πρέπει να έχουμε $A_4(3, 2) \leq 4^{3-2+1} = 16$. Δηλαδή τελικά έχουμε ισότητα.

Θεώρημα 1.5.22. *Έστω $\mathcal{C}$ ένας (n, M, d) κώδικας επί του αλφάβητου $\mathbb{A} = \{\, a_0, a_1, \ldots, a_{r-1} \,\}$. Υποθέτουμε ότι $d > \vartheta \cdot n$, όπου $\vartheta = \frac{r-1}{r}$. Για το μέγεθος M του κώδικα ισχύει $M \leq \frac{d}{d-\vartheta \cdot n}$.*

Απόδειξη. Έστω $S = \sum d(\mathbf{x}, \mathbf{y})$, όπου το άθροισμα εκτείνεται σε όλα τα διατεταγμένα ζεύγη $(\mathbf{x}, \mathbf{y})$ (διαφορετικών μεταξύ τους) (κωδικο)λέξεων. Το πλήθος αυτών των ζευγών ως γνωστόν είναι ίσο με $2\binom{M}{2} = M(M-1)$ και επειδή η απόσταση μεταξύ δύο (διαφορετικών) (κωδικο)λέξεων είναι τουλάχιστον ίση με d, έχουμε ότι $S \geq M(M-1)d$.

Θα υπολογίσουμε τώρα ένα άνω φράγμα για το άθροισμα S. Σχηματίζουμε έναν $M \times n$ πίνακα του οποίου οι γραμμές είναι τα στοιχεία του $\mathcal{C}$

$$\begin{array}{cccccc} \mathbf{c}_1 & = & c_{11} & c_{12} & \cdots & c_{1n} \\ \mathbf{c}_2 & = & c_{21} & c_{22} & \cdots & c_{2n} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \mathbf{c}_M & = & c_{M1} & c_{M2} & \cdots & c_{Mn} \end{array} .$$

Επιλέγουμε μία (τυχαία) στήλη του πίνακα και έναν τυχαίο χαρακτήρα $a \in \mathbb{A}$. Έστω m_a το πλήθος των εμφανίσεων του χαρακτήρα a σ' αυτή τη στήλη, τότε προφανώς $\sum_{a \in \mathbb{A}} m_a = M$, επίσης σε $M - m_a$ το πλήθος από τις (κωδικο)λέξεις σ' αυτή τη στήλη εμφανίζεται ένας άλλος χαρακτήρας διαφορετικός από τον a. Επομένως η *συμβολή* αυτής της στήλης στο άθροισμα των αποστάσεων όλων των διατεταγμένων ζευγών (διαφορετικών μεταξύ τους) (κωδικο)λέξεων είναι ίση με $\sum_{a \in \mathbb{A}} m_a(M - m_a) = M^2 - \sum_{a \in \mathbb{A}} m_a^2$. Η διαδικασία αυτή επαναλαμβάνεται για όλες (n το πλήθος) στήλες του πίνακα, οπότε έχουμε $S \leq n(M^2 - \sum_{a \in \mathbb{A}} m_a^2)$. Το άθροισμα $\sum_{a \in \mathbb{A}} m_a^2$ λαμβάνει την ελάχιστη τιμή αν όλα τα m_a είναι ίσα με M/r (γιατί;). Επομένως από την προηγούμενη σχέση έχουμε ότι $S \leq n(M^2 - M^2/r)$.

Συνδυάζοντας το κάτω φράγμα του S, που βρήκαμε παραπάνω με την τελευταία σχέση, έχουμε $M(M-1)d \leq S \leq n(M^2 - M^2/r)$. Αγνοώντας το S και λύνοντας ως προς M έχουμε την αποδεικτέα σχέση.

□

Πόρισμα 1.5.23. (Φράγμα Plotkin) *Δεδομένου ότι ισχύει $d > \vartheta \cdot n$ έχουμε $A_r(n, d) \leq \frac{d}{d-\vartheta \cdot n}$.*

Όπως παρατηρούμε το άνω φράγμα Plotkin εφαρμόζεται όταν ο κώδικας είναι αρκετά *αραιός*. Στην περίπτωση μάλιστα που το μέγεθος r του αλφαβήτου είναι πολύ μεγάλο, τότε το $\vartheta = \frac{r-1}{r}$ *πλησιάζει* να γίνει 1, οπότε, για να εφαρμόσουμε το προηγούμενο πόρισμα, η ελάχιστη απόσταση του κώδικα πρέπει να είναι *σχεδόν* ίση με το μήκος n του κώδικα.

Ενδιαφέρον παρουσιάζει η περίπτωση των δυαδικών κωδίκων, όπου εκεί $\vartheta = \frac{r-1}{r} = \frac{1}{2}$. Εδώ θα δούμε πώς το προηγούμενο αποτέλεσμα εφαρμόζεται ακόμα και σε περιπτώσεις, όπου δεν ισχύει κατ' ανάγκη $d > \frac{1}{2}n$, διακρίνοντας αν η ελάχιστη απόσταση είναι άρτια ή περιττή.

Θεώρημα 1.5.24. (Το φράγμα Plotkin σε δυαδικούς κώδικες)
Έστω $\mathcal{C}$ ένας δυαδικός (n, M, d) κώδικας.

1. Υποθέτουμε ότι η ελάχιστη απόσταση d είναι άρτια, τότε για $d > \frac{1}{2}n$ έχουμε $A_2(n, d) \leq 2\lfloor \frac{d}{2d-n} \rfloor$ και
για $n = 2d$ (οπότε $d = \frac{1}{2}n$) έχουμε $A_2(2d, d) \leq 4d$.

2. Υποθέτουμε ότι η ελάχιστη απόσταση d είναι περιττή, τότε για $d > \frac{1}{2}(n-1)$ έχουμε $A_2(n, d) \leq 2\lfloor \frac{d+1}{2d+1-n} \rfloor$ και
για $d = \frac{1}{2}(n-1)$ έχουμε $A_2(2d+1, d) \leq 4(d+1)$.

Απόδειξη. 1. Αν $d > \frac{1}{2}n$, τότε στο προηγούμενο πόρισμα απλώς θέτουμε $\vartheta = \frac{1}{2}$ και έχουμε $A_2(n, d) \leq 2\lfloor \frac{d}{2d-n} \rfloor$.

Στην περίπτωση, όπου $d = 2k$ και $n = 2d = 4k$, από το Θεώρημα 1.5.16 έχουμε $A_2(n, d) = A_2(4k, 2k) \leq 2A_2(4k-1, 2k)$. Εφαρμόζοντας τώρα το προηγούμενο αποτέλεσμα η προηγούμενη σχέση συνεχίζεται $A_2(n, d) = A_2(4k, 2k) \leq 2A_2(4k-1, 2k) \leq 4\lfloor \frac{2k}{4k-(4k-1)} \rfloor = 8k = 4d$.

2. Εδώ έχουμε υποθέσει ότι η ελάχιστη απόσταση είναι περιττή. Από το Θεώρημα 1.5.14 έχουμε ότι $A_2(n, d) = A_2(n+1, d+1) \leq 2\lfloor \frac{d+1}{2d+1-n} \rfloor$.

Στην περίπτωση όπου $d = \frac{1}{2}(n-1)$, δηλαδή $n = 2d+1$, έχουμε, πάλι από το Θεώρημα 1.5.14 και τη δεύτερη σχέση της πρώτης περίπτωσης (αφού $d+1$ είναι άρτιος), ότι $A_2(n, d) = A_2(n+1, d+1) = A_2(2d+2, d+1) \leq 4(d+1)$. □

Παρατήρηση 1.5.25. Όπως είδαμε στην προηγούμενη απόδειξη τα Θεωρήματα 1.5.14 και 1.5.16 είναι πολύ χρήσιμα στην εφαρμογή του φράγματος Plotikin και στην περίπτωση όπου $d \leq \frac{r-1}{r}n$. Εδώ αρκούμαστε σε ένα επιπλέον παράδειγμα, όπου εφαρμόζουμε διαδοχικά το Θεώρημα 1.5.16.

$A_2(13, 5) = 2^3 A_2(10, 5) \leq 8 \cdot 2\lfloor \frac{6}{11-10} \rfloor = 96$.

1.5.3 Ασκήσεις

1. Έστω $\mathcal{C}$ ένας κώδικας, ο οποίος δεν είναι βέλτιστος, είναι δυνατόν να επισυνάψουμε στοιχεία στον $\mathcal{C}$ έτσι ώστε να προκύψει ένας βέλτιστος κώδικας;

2. Έστω $\mathbb{A}$ ένα αλφάβητο και $\mathbf{a}, \mathbf{b} \in \mathbb{A}^n$. Δείξτε ότι τα σύνολα $S = \{\, \mathbf{x} \in \mathbb{A}^n \mid d(\mathbf{x}, \mathbf{a}) < d(\mathbf{x}, \mathbf{b}) \,\}$ και $T = \{\, \mathbf{x} \in \mathbb{A}^n \mid d(\mathbf{x}, \mathbf{b}) < d(\mathbf{x}, \mathbf{a}) \,\}$ έχουν το ίδιο πλήθος στοιχείων.

3. Δείξτε ότι, για $d_1 \geq d_2$, ισχύει: $A_r(n, d_1) \leq A_r(n, d_2)$.

4. Υπάρχει δυαδικός κώδικας με παραμέτρους $(8, 29, 3)$;

5. Να υπολογίσετε το κάτω και άνω φράγμα που αναφέρονται στο Θεώρημα 1.5.18 για τις ακόλουθες περιπτώσεις: $A_2(7, 3)$, $A_2(10, 5)$, $A_2(13, 7)$, $A_2(14, 7)$, $A_2(15, 7)$. Συγκρίνετε με τις τιμές του πίνακα της σελίδας 51.

6. Να συγκρίνετε τα τρία άνω φράγματα Hamming, Singleton, Plotkin στις ακόλουθες περιπτώσεις:
$A_2(7, 5)$, $A_2(8, 5)$, $A_2(9, 5)$, $A_2(15, 9)$.

7. Δείξτε ότι $A_{10}(10, 3) \leq 100.000.000$.

8. Δείξτε ότι $A_r(r+1, 3) \leq r^{r-1}$ και $A_r(r+1, 5) \leq \frac{2r^{r-2}}{r-1}$.

9. Δείξτε ότι αν το d είναι ίσο με μια δύμανη του 2, τότε $A_2(2d, d) = 4d$.

10. Έστω $\mathcal{C}$ ένας τέλειος δυαδικός κώδικας με παραμέτρους $(n, M, 7)$. Δείξτε ότι $n = 7$ ή $n = 23$.

Κεφάλαιο 2

Γραμμικοί Κώδικες

2.1 Η έννοια του Γραμμικού κώδικα.

Μέχρι τώρα θεωρούσαμε έναν (n, M, d) κώδικα $\mathcal{C}$ απλώς σαν ένα υποσύνολο του συνόλου $\mathbb{A}^n$, όπου $\mathbb{A}$ είναι ένα αλφάβητο. Είχαμε, όμως πει ότι συνήθως ως αλφάβητο θεωρούμε το σύνολο $\mathbb{A} = \mathbb{Z}_p$ των ακεραίων $\mod p$, όπου p είναι ένας πρώτος αριθμός, το οποίο είναι σώμα. Στην περίπτωση όμως αυτή το σύνολο $\mathbb{A}^n$ έχει αλγεβρική δομή, είναι διανυσματικός χώρος επί του σώματος $\mathbb{Z}_p$. Επομένως λογικό είναι να απαιτήσουμε ένας κώδικας, σαν υποσύνολο του $\mathbb{A}^n$, να έχει και αυτός αλγεβρική δομή, να είναι διανυσματικός υπόχωρος του $\mathbb{A}^n$.

Ορισμός 2.1.1. *Έστω $\mathbb{F}_p$ ένα πεπερασμένο σώμα (π.χ. $\mathbb{F}_p = \mathbb{Z}_p$, όπου p πρώτος), το οποίο στο εξής θα το θεωρούμε ως αλφάβητο, ένας κώδικας $\mathcal{C} \subseteq \mathbb{F}_p^n$ θα λέγεται* **γραμμικός** *αν είναι διανυσματικός υπόχωρος του διανυσματικού χώρου $\mathbb{F}_p^n$.* [1]

Παραδείγματα 2.1.2.

1. Ο δυαδικός κώδικας $\mathcal{C} = \{\, 0000,\ 1011,\ 0110,\ 1101 \,\} \subseteq \mathbb{Z}_2^4$ είναι γραμμικός (γιατί;).

2. Ο δυαδικός κώδικας $\mathcal{C} = \{\, 0001,\ 1011,\ 0110,\ 1111 \,\} \subseteq \mathbb{Z}_2^4$ δεν είναι γραμμικός (γιατί;).

3. Το σύνολο $\mathrm{B} = \{\, 1000011,\ 0100101,\ 0010110,\ 0001111 \,\}$ είναι γραμμικά ανεξάρτητο επί του $\mathbb{Z}_2$ (γιατί;). Επομένως παράγει ένα δυαδικό γραμμικό κώδικα διάστασης 4.

[1] Στα επόμενα, όπου το αλφάβητο ενός κώδικα είναι ένα πεπερασμένο σώμα με πλήθος στοιχείων μια δύναμη του p, θα χρησιμοποιούμε τον συμβολισμό $\mathbb{F}_p$.

4. Ο n-επαναληπτικός κώδικας $\mathcal{R}_r(n)$ $r-$αδικός κώδικας είναι ένας γραμμικός κώδικας διάστασης ένα για οποιοδήποτε μήκος n και για οποιοδήποτε πεπερασμένο σώμα ως αλφάβητο (γιατί;).

5. Έστω $\mathcal{E}_n$ το υποσύνολο του $\mathbb{F}_p^n$ που αποτελείται από όλες τις λέξεις $\mathbf{c} = c_1c_2\cdots c_n \in \mathbb{F}_p^n$ των οποίων το άθροισμα των χαρακτήρων ισούται με μηδέν, δηλαδή $\sum_{i=1}^{n} c_i = 0$. Δεν είναι δύσκολο να δούμε ότι το $\mathcal{E}_n$ είναι ένας γραμμικός κώδικας. Προφανώς κάθε κώδικας μηδενικού αθροίσματος είναι υποσύνολο του $\mathcal{E}_n$.

Έστω k η διάσταση ενός γραμμικού κώδικα $\mathcal{C}$ ως διανυσματικού χώρου. Τότε, ως γνωστόν, το μέγεθός του είναι ίσο με $\mid \mathcal{C} \mid = q^k$, όπου q είναι το πλήθος του αλφάβητου (σώματος) $\mathbb{F}_p$. Δηλαδή η διάσταση ενός γραμμικού κώδικα καθορίζει και το μέγεθός του. Επομένως στη συνέχεια, όταν αναφερόμαστε στις παραμέτρους ενός γραμμικού κώδικα αντί να λέμε ο κώδικας $(n,\, q^k,\, d)$, θα λέμε ο κώδικας $[n,\, k,\, d]$.
(Προσοχή στο συμβολισμό οι παρενθέσεις γίνονται αγκύλες, όταν αντί για το μέγεθος του κώδικα χρησιμοποιούμε την διάστασή του. Επίσης δεν σημαίνει ότι κάθε κώδικας μεγέθους μιας δύναμης ενός πρώτου αριθμού είναι γραμμικός).

Σημείωση: Ο μηδενικός κώδικας (που αποτελείται μόνο από τη μηδενική (κωδικο)λέξη) είναι προφανώς γραμμικός κώδικας με διάσταση μηδέν. Στα επόμενα θα θεωρούμε, χωρίς ιδιαίτερη μνεία, μη μηδενικούς γραμμικούς κώδικες.

Το ότι ένας κώδικας είναι γραμμικός είναι πολύ σημαντικό, γι' αυτό, όπως θα δούμε παρακάτω, οι περισσότεροι *καλοί* κώδικες είναι γραμμικοί. Ως μια πρώτη συνέπεια της γραμμικότητας ενός κώδικα έχουμε.

Θεώρημα 2.1.3. *Έστω $\mathcal{C}$ ένας γραμμικός κώδικας. Η ελάχιστη απόστασή του ισούται με την ελάχιστη απόσταση των (κωδικο)λέξεων από τη μηδενική (κωδικο)λέξη $\mathbf{0}$. Δηλαδή $d(\mathcal{C}) = \min\{\, d(\mathbf{c},\, \mathbf{0}), \mathbf{c} \in \mathcal{C}\,\}$.*

Απόδειξη. Προφανώς (γιατί προφανώς;) ισχύει $d(\mathcal{C}) \leq \min\{\, d(\mathbf{c},\, \mathbf{0}), \mathbf{c} \in \mathcal{C}\backslash\{\,\mathbf{0}\,\}\,\}$.

Αντίστροφα, έστω $\mathbf{a}$, $\mathbf{b}$ δύο (κωδικο)λέξεις, τότε, ως γνωστόν, $d(\mathbf{a},\, \mathbf{b}) = d(\mathbf{a} - \mathbf{b},\, \mathbf{0}) \geq \min\{\, d(\mathbf{c},\, \mathbf{0}), \mathbf{c} \in \mathcal{C}\,\}$, διότι η διαφορά $\mathbf{c} = \mathbf{a} - \mathbf{b}$ ανήκει στο κώδικα $\mathcal{C}$, αφού ο κώδικας είναι γραμμικός.

□

Η ελάχιστη απόσταση των λέξεων ενός γραμμικού κώδικα από τη μηδενική λέξη λέγεται **ελάχιστο βάρος** του κώδικα και συμβολίζεται $w(\mathcal{C})$. Δηλαδή $w(\mathcal{C}) = \min\{\, d(\mathbf{c},\, \mathbf{0}), \mathbf{c} \in \mathcal{C}\backslash\{\,\mathbf{0}\,\}\,\}$.

Το προηγούμενο θεώρημα έχει μεγάλη σημασία στην πράξη. Αρκεί να αναλογιστούμε την οικονομία χρόνου που επιτυγχάνουμε για τον υπολογισμό της

ελάχιστης απόστασης ενός γραμμικού κώδικα μεγέθους M. Αντί για τον υπολογισμό της απόστασης $\binom{M}{2}$ ζευγών λέξεων, αρκεί να υπολογίσουμε μόνο την απόσταση $M-1$ ζευγών λέξεων. Για παράδειγμα, υπολογίστε την ελάχιστη απόσταση στα προηγούμενα παραδείγματα γραμμικών κωδίκων.

Στη σελίδα 39 είχαμε δεί πώς πέρνουμε μια αύξηση ενός δυαδικού κώδικα $\mathcal{C}$ επισυνάπτοντας το συμπλήρωμά του. Στην περίπτωση, όπου ο κώδικας $\mathcal{C}$ είναι γραμμικός, έχουμε ότι και ο κώδικας $\mathcal{C} \cup \mathcal{C}^c$ είναι γραμμικός. Συγκεκριμένα έχουμε.

Πρόταση 2.1.4. *Έστω $\mathcal{C}$ ένας (n, M, d) δυαδικός γραμμικός κώδικας. Αν η λέξη $\mathbf{1} = 11\cdots1$ ανήκει στον κώδικα $\mathcal{C}$, τότε $\mathcal{C} = \mathcal{C}^c$.*

Αν η λέξη $\mathbf{1} = 11\cdots1$ δεν ανήκει στον κώδικα $\mathcal{C}$, τότε $\mathcal{C} \cap \mathcal{C}^c = \emptyset$ και το $\mathcal{C} \cup \mathcal{C}^c$ είναι $(n, 2M, \bar{d})$ γραμμικός κώδικας, όπου
$\bar{d} = min\{\, d(\mathcal{C}),\ n - max\{\, d(\mathbf{c}, \mathbf{d}),\ \mathbf{c}, \mathbf{d} \in \mathcal{C}\,\}\,$.

Απόδειξη. Η απόδειξη είναι εύκολη και αφίνεται ως άσκηση, αρκεί να ανατρέξουμε στη σελίδα 39 και παράλληλα να εφαρμόσουμε τον ορισμό του γραμμικού κώδικα. □

2.1.1 Γεννήτορες πίνακες ενός Γραμμικού κώδικα.

Έστω $\mathcal{C}$ ένας $[n, k, d]$ γραμμικός κώδικας επί του σώματος $\mathbb{F}_p$. Ως διανυσματικός υπόχωρος του $\mathbb{F}_p^n$ έχει μια βάση $\mathbf{B} = \{\, \mathbf{b_1}, \mathbf{b_2}, \ldots, \mathbf{b_k}\,\}$. Για κάθε (κωδικο)λέξη $\mathbf{c}$ υπάρχουν (μοναδικά) $\lambda_1, \lambda_2, \ldots, \lambda_k \in \mathbb{F}_p$ έτσι ώστε $\mathbf{c} = \lambda_1\mathbf{b_1} + \lambda_2\mathbf{b_2} + \cdots + \lambda_k\mathbf{b_k}$. Αντίστροφα για κάθε $\mathbf{r} = (\lambda_1, \lambda_2, \ldots, \lambda_k) \in \mathbb{F}_p^k$ το στοιχείο $\lambda_1\mathbf{b_1} + \lambda_2\mathbf{b_2} + \cdots + \lambda_k\mathbf{b_k}$ ανήκει στον κώδικα $\mathcal{C}$.

Έστω τώρα ο $k \times n$ πίνακας G, του οποίου οι γραμμές αποτελούνται από τα στοιχεία της βάσης $\mathbf{B}$, τότε, εφαρμόζοντας τον ορισμό του πολλαπλασιασμού πινάκων, από τα προηγούμενα έχουμε ότι $\mathcal{C} = \{\, \mathbf{r} \cdot \mathrm{G} \mid \mathbf{r} \in \mathbb{F}_p^k\,\}$.

Ορισμός 2.1.5. *Έστω $\mathcal{C}$ ένας $[n, k, d]$ γραμμικός κώδικας επί του σώματος $\mathbb{F}_p$, ένας $k \times n$ πίνακας του οποίου οι γραμμές αποτελούν μια βάση του $\mathcal{C}$ ονομάζεται* **γεννήτορας πίνακας** *του $\mathcal{C}$.*

Παραδείγματα 2.1.6.

1. Ένας γεννήτορας πίνακας του δυαδικού γραμμικού κώδικα $\mathcal{C} = \{\, 0000, 1011, 0110, 1101\,\} \subseteq \mathbb{Z}_2^4$ είναι ο πίνακας $\mathrm{G} = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}$ (γιατί;).

2. Το σύνολο $\mathrm{B} = \{\, 1000011, 0100101, 0010110, 0001111\,\}$ είναι γραμμικά ανεξάρτητο επί του $\mathbb{Z}_2$ (γιατί;). Επομένως ο παραγόμενος δυαδικός γραμ-

μικός κώδικας έχει ως γεννήτορα πίνακα τον πίνακα

$$\mathrm{G} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

3. Ο $n-$επαναληπτικός κώδικας $\mathcal{R}_r(n)$ $r-$αδικός κώδικας έχει ως γεννήτορα πίνακα τον $1 \times n$ πίνακα $\mathrm{G} = \begin{pmatrix} 1 & 1 & \cdots & 1 \end{pmatrix}$ (γιατί;).

Προφανώς σε έναν γραμμικό κώδικα, όταν λαμβάνουμε μια άλλη βάση, τότε έχουμε και έναν άλλο γεννήτορα πίνακα.

Από την Γραμμική Άλγεβρα είναι γνωστό το επόμενο αποτέλεσμα, που αναφέρεται στο πώς σχετίζονται δύο γεννήτορες πίνακες ενός γραμμικού κώδικα.

Λήμμα 2.1.7. *Έστω $\mathcal{C}$ ένας $[n, k, d]$ γραμμικός κώδικας και* R *ένας $k \times k$ αντιστρέψιμος πίνακας με στοιχεία από το αλφάβητο $\mathbb{F}_p$. Τότε για κάθε γεννήτορα πίνακα* G *του κώδικα, το γινόμενο* RG *είναι γεννήτορας πίνακας του κώδικα. Αντίστροφα, έστω* G_1 *και* G_2 *δύο γεννήτορες πίνακες του κώδικα, τότε υπάρχει ένας $k \times k$ αντιστρέψιμος πίνακας* R *με στοιχεία από το αλφάβητο $\mathbb{F}_p$, τέτοιος ώστε* $\mathrm{G}_2 = \mathrm{RG}_1$.

Απόδειξη. Έστω $\{ \mathbf{b_1}, \mathbf{b_2}, \ldots, \mathbf{b_k} \}$ μία βάση του $\mathcal{C}$ της οποίας τα στοιχεία αποτελούν τις γραμμές του γεννήτορα πίνακα G. Δηλαδή $\mathrm{G} = \begin{pmatrix} \mathbf{b_1} \\ \mathbf{b_2} \\ \vdots \\ \mathbf{b_k} \end{pmatrix}$. Επίσης έστω ο αντιστρέψιμος πίνακας $\mathrm{R} = (\lambda_{ij})_{k \times k}$. Τότε η $i-$γραμμή του γινομένου RG είναι ίση με $\lambda_{i1}\mathbf{b_1} + \lambda_{i2}\mathbf{b_2} + \cdots + \lambda_{ik}\mathbf{b_k}$. Επομένως οι γραμμές του πίνακα RG παράγουν έναν υπόχωρο του $\mathcal{C}$. Αλλά ως γνωστόν η τάξη του γινομένου RG είναι μικρότερη ή ίση από την τάξη του πίνακα G. Επίσης η τάξη του πίνακα $\mathrm{G} = \mathrm{R}^{-1}(\mathrm{RG})$ είναι μικρότερη ή ίση από την τάξη του πίνακα RG, άρα οι δύο πίνακες G και RG έχουν την ίδια τάξη. Δηλαδή οι γραμμές του πίνακα είναι γραμμικώς ανεξάρτητες και επομένως ο υπόχωρος του $\mathcal{C}$ που παράγουν είναι ολόκληρος ο κώδικας $\mathcal{C}$. Άρα ο πίνακας RG είναι γεννήτορας πίνακας του κώδικα.

Αντίστροφα, έστω G_1 και G_2 δύο γεννήτορες πίνακες του κώδικα οι γραμμές των οποίων αποτελούν βάσεις του κώδικα. Δηλαδή $\mathrm{G}_1 = \begin{pmatrix} \mathbf{b_1} \\ \mathbf{b_2} \\ \vdots \\ \mathbf{b_k} \end{pmatrix}$ και

$\mathrm{G}_2 = \begin{pmatrix} \mathbf{c_1} \\ \mathbf{c_2} \\ \vdots \\ \mathbf{c_k} \end{pmatrix}$. Εκφράζουμε τα στοιχεία της βάσης $\{\mathbf{c_1}, \mathbf{c_2}, \ldots, \mathbf{c_k}\}$ ως γραμμικό συνδυασμό των στοιχείων της βάσης $\{\mathbf{b_1}, \mathbf{b_2}, \ldots, \mathbf{b_k}\}$. Δηλαδή $\mathbf{c_i} = \lambda_{i1}\mathbf{b_1} + \lambda_{i2}\mathbf{b_2} + \cdots + \lambda_{ik}\mathbf{b_k}$ για $i = 1, 2, \ldots, k$. Ο $k \times k$ πίνακας $\mathrm{R} = (\lambda_{ij})$ προφανώς έχει την ιδιότητα $\mathrm{G}_2 = \mathrm{RG}_1$ και επιπλέον είναι αντιστρέψιμος, αφού αποτελεί τον πίνακα αλλαγής βάσης.

□

Παράδειγμα 2.1.8. Για τους κώδικες που αναφέρονται στα τρία προηγούμενα παραδείγματα μπορείτε να κατασκευάσετε άλλους γεννήτορες πίνακες εφαρμόζοντας το προηγούμενο Λήμμα.

Έστω $\mathcal{C}$ ένας $[n, k, d]$ γραμμικός κώδικας και $\sigma \in S_n$ μια μετάθεση $n-$συμβόλων. Εφαρμόζοντας την σ στους χαρακτήρες κάθε (κωδικο)λέξης
$\mathbf{c} = (a_1, a_2, \ldots, a_n) \in \mathcal{C}$ λαμβάνουμε, ως γνωστόν έναν ισοδύναμο κώδικα, έστω $\mathcal{C}_\sigma$. Δηλαδή $\mathcal{C}_\sigma = \{\sigma(\mathbf{c}) = (a_{\sigma(1)}, a_{\sigma(2)}, \ldots, a_{\sigma(n)}) \mid \mathbf{c} \in \mathcal{C}\}$.

Έστω τώρα ο πίνακας P_σ μετάθεση, ο οποίος προκύπτει από τον ταυτοτικό πίνακα $\mathrm{I}_{n\times n}$ αν εφαρμόσουμε μια μετάθεση $\sigma \in S_n$ στις γραμμές του. Προφανώς ο πίνακας P_σ είναι αντιστρέψιμος (έχει τάξη n). Δεν είναι δύσκολο να δούμε ότι για κάθε $\mathbf{c} = (a_1, a_2, \ldots, a_n) \in \mathcal{C}$ ισχύει $(a_1, a_2, \ldots, a_n)\,\mathrm{P}_\sigma = (a_{\sigma(1)}, a_{\sigma(2)}, \ldots, a_{\sigma(n)})$. Δηλαδή $\mathcal{C}_\sigma = \{\mathbf{c}\,\mathrm{P}_\sigma \mid \mathbf{c} \in \mathcal{C}\}$. Αυτό είναι ισοδύναμο με το ότι αν ο πίνακας G είναι γεννήτορας πίνακας του κώδικα $\mathcal{C}$, τότε ο πίνακας GP_σ είναι γεννήτορας πίνακας του κώδικα $\mathcal{C}_\sigma$.

Από τα προηγούμενα έπεται η επόμενη πρόταση.

Πρόταση 2.1.9. *Έστω $\mathcal{C}$ ένας $[n, k, d]$ γραμμικός κώδικας και $\sigma \in S_n$ μια μετάθεση $n-$συμβόλων. Τότε και ο ισοδύναμος κώδικας $\mathcal{C}_\sigma$ είναι γραμμικός.*

Απόδειξη. Είναι εύκολο να ελέγξουμε ότι ο κώδικας $\mathcal{C}_\sigma$ είναι ένας διανυσματικός χώρος, αφού ο $\mathcal{C}$ είναι διανυσματικός χώρος (άσκηση).

Διαφορετικά θα μπορούσαμε να πούμε. Ως γνωστόν σε κάθε πίνακα αντιστοιχεί μια γραμμική απεικόνιση (γιατί;), και γραμμικές απεικονίσεις απεικονίζουν διανυσματικούς χώρους σε διανυσματικούς χώρους.

□

Ως γνωστόν οι ισοδύναμοι κώδικες $\mathcal{C}$ και $\mathcal{C}_\sigma$ έχουν τις ίδιες παραμέτρους (μήκος, μέγεθος και ελάχιστη απόσταση). Δηλαδή είναι *εξ' ίσου αποτελεσματικοί*, επομένως το επόμενο αποκτά ιδιαίτερη σημασία στη θεωρία των γραμμικών κωδίκων.

Θεώρημα 2.1.10. *Έστω $\mathcal{C}$ ένας $[n, k, d]$ γραμμικός κώδικας. Τότε υπάρχει ένας ισοδύναμος γραμμικός κώδικας $\bar{\mathcal{C}}$, ο οποίος έχει ως γεννήτορα πίνακα ένα $k \times n$ πίνακα του οποίου οι k πρώτες στήλες σχηματίζουν τον ταυτοτικό πίνακα I_k.*

Απόδειξη. Έστω G ένας γεννήτορας πίνακας του κώδικα $\mathcal{C}$. Ο πίνακας αυτός έχει k το πλήθος γραμμικώς ανεξάρτητες στήλες. Έστω $\sigma \in S_n$ μια μετάθεση, η οποία μεταθέτει τις στήλες του πίνακα G κατά τέτοιο τρόπο ώστε οι k το πλήθος γραμμικώς ανεξάρτητες στήλες να καταλάβουν τις k πρώτες θέσεις στις στήλες του πίνακα G. Έστω P ο πίνακας της μετάθεσης σ και M ο πίνακας που προκύπτει από τον πίνακα G σύμφωνα με την προηγούμενη διαδικασία. Τότε είναι εύκολο να παρατηρήσουμε ότι ισχύει $\mathrm{M} = \mathrm{GP}$ (γιατί;).

Έστω $\bar{\mathcal{C}}$ ο γραμμικός κώδικας που έχει ως γεννήτορα πίνακα τον πίνακα M. Δηλαδή $\bar{\mathcal{C}} = \{ (\lambda_1, \lambda_2, \ldots, \lambda_k)\cdot\mathrm{M} \mid (\lambda_1, \lambda_2, \ldots, \lambda_k) \in \mathbb{A}^k \} = \{ (\lambda_1, \lambda_2, \ldots, \lambda_k)\cdot \mathrm{GP} \mid (\lambda_1, \lambda_2, \ldots, \lambda_k) \in \mathbb{A}^k \} = \{ \mathbf{c}\mathrm{P} \mid \mathbf{c} \in \mathcal{C} \}$. Ο κώδικας $\bar{\mathcal{C}}$ είναι ισοδύναμος ως προς τον κώδικα $\mathcal{C}$ και οι k πρώτες στήλες του γεννήτορα πίνακα M είναι γραμμικώς ανεξάρτητες. Έστω R ο $k \times k$ (υπο)πίνακας που σχηματίζουν k πρώτες στήλες του πίνακα M και S ο $k \times n-k$ (υπο)πίνακας που σχηματίζουν $n-k$ υπόλοιπες στήλες του πίνακα M. Δηλαδή ο πίνακας M έχει τη μορφή $\mathrm{M} = [\mathrm{R} \quad \mathrm{S}]$. Ο πίνακας R είναι αντιστρέψιμος (γιατί;), επομένως από το λήμμα 2.1.7 έχουμε ότι ο πίνακας $\mathrm{R}^{-1}\mathrm{M}$ είναι γεννήτορας πίνακας του κώδικα $\bar{\mathcal{C}}$. Αλλά $\mathrm{R}^{-1}\mathrm{M} = \mathrm{R}^{-1}[\mathrm{R} \quad \mathrm{S}] = [\mathrm{R}^{-1}\mathrm{R} \quad \mathrm{R}^{-1}\mathrm{S}] = [\mathrm{I}_k \quad \mathrm{R}^{-1}\mathrm{S}]$.

Ο πίνακας $\mathrm{N} = [\mathrm{I}_k \quad \mathrm{R}^{-1}\mathrm{S}]$ είναι ο γεννήτορας πίνακας του κώδικα $\bar{\mathcal{C}}$ με την απαιτούμενη ιδιότητα.

□

Ορισμός 2.1.11. *Ένας $k \times n$ πίνακας* A *με τάξη k θα λέγεται* **ανηγμένος κλιμακωτός** *αν είναι της μορφής* $\mathrm{A} = [\mathrm{I}_k \quad \mathrm{B}]$.

Τα προηγούμενα συνοψίζονται στο επόμενο πόρισμα.

Πόρισμα 2.1.12. *Για κάθε γραμμικό κώδικα υπάρχει ένας ισοδύναμος γραμμικός κώδικας με γεννήτορα πίνακα ένα ανηγμένο κλιμακωτό πίνακα.*

Όπως έχουμε επισημάνει ισοδύναμοι κώδικες έχουν τις ίδιες παραμέτρους, επομένως έχουν την ίδια αποτελεσματικότητα στην ανίχνευση/διόρθωση λαθών. Για το λόγο αυτό πολλές φορές είναι προτιμότερο, αντί του αρχικού κώδικα, να εργαζόμαστε με έναν ισοδύναμο κώδικα που έχει γεννήτορα πίνακα σε ανηγμένη κλιμακωτή μορφή. Σαν παράδειγμα θα δώσουμε μια άλλη απόδειξη του φράγματος Singleton (Θεώρημα 1.5.20) στην περίπτωση των γραμμικών κωδίκων.

Πρόταση 2.1.13. *Αν $\mathcal{C}$ είναι ένας $[n, k, d]$ γραμμικός κώδικας, τότε $d \leq n - k + 1$.*

Απόδειξη. Από τα προηγούμενα μπορούμε να υποθέσουμε ότι ο κώδικας έχει γεννήτορα πίνακα G σε ανηγμένη κλιμακωτή μορφή. Δηλαδή $G = [\mathrm{I}_k \quad \mathrm{B}]$. Κάθε γραμμή του πίνακα G είναι μια (κωδικο)λέξη με 0 σε τουλάχιστον $k-1$ το πλήθος θέσεις. Επομένως έχει βάρος το πολύ ίσον με $n-(k-1)$. Οπότε από το Θεώρημα 2.1.3 έχουμε ότι $d \leq n-k+1$.

□

Έστω $\mathcal{C}$ ένας $[n,\, k,\, d]$ γραμμικός κώδικας με γεννήτορα πίνακα $\mathrm{G} = [\mathrm{I}_k \quad \mathrm{A}]$ σε ανηγμένη κλιμακωτή μορφή. Επειδή
$\mathcal{C} = \{\, (\lambda_1, \lambda_2, \ldots, \lambda_k)\cdot \mathrm{G} \mid (\lambda_1, \lambda_2, \ldots, \lambda_k) \in \mathbb{A}^k \,\}$, κάθε (κωδικο)λέξη μπορεί να χωρισθεί σε δύο τμήματα. Το πρώτο τμήμα που αποτελείται από τους k πρώτους χαρακτήρες μπορεί να είναι οποιοδήποτε στοιχείο $(\lambda_1, \lambda_2, \ldots, \lambda_k) \in \mathbb{A}^k$, ενώ το υπόλοιπο τμήμα της των $n-k$ χαρακτήρων προσδιορίζεται από το πρώτο τμήμα βάσει του κανόνα $(\lambda_1, \lambda_2, \ldots, \lambda_k)\,\mathrm{A}$. Για το λόγο αυτό συνήθως το πρώτο τμήμα το ονομάζουμε **τμήμα πληροφορίας** και το υπόλοιπο το ονομάζουμε **τμήμα ελέγχου ισοτιμίας**. Καθότι οι k πρώτοι χαρακτήρες *περικλείουν* τη μεταδιδόμενη πληροφορία, ενώ οι υπόλοιποι $n-k$ χαρακτήρες *ελέγχουν* τη σωστή μετάδοση της πληροφορίας. Γενικά τέτοιοι κώδικες ονομάζονται **συστηματικοί κώδικες** ή **διαχωρίσιμοι κώδικες** .

Η χρήση συστηματικών κωδίκων προσφέρει πολλά πλεονεκτήματα. Αρκεί να αναλογισθούμε την οικονομία χρόνου που επιτυγχάνουμε καθότι μπορούμε να αποστέλλουμε το τμήμα πληροφορίας, ενώ ταυτόχρονα υπολογίζουμε το τμήμα ελέγχου ισοτιμίας.

Υπάρχει μια διαδικασία (αλγόριθμος) με την οποία, για δεδομένο γραμμικό κώδικα, μπορούμε να προδιορίσουμε τον αντίστοιχο ισοδύναμο κώδικα του οποίου ο γεννήτορας πίνακας είναι σε ανηγμένη κλιμακωτή μορφή.

Έστω ένας $m \times n$ πίνακας A με στοιχεία από ένα σώμα $\mathbb{F}$, στις γραμμές και στις στήλες του πίνακα μπορούμε να πραγματοποιήσουμε τους εξής μετασχηματισμούς.

1. Να αντιμεταθέσουμε δύο γραμμές του πίνακα.
2. Να πολλαπλασιάσουμε μια γραμμή του πίνακα με ένα μη μηδενικό στοιχείο του σώματος.
3. Να προσθέσουμε ένα πολλαπλάσιο μιας γραμμής σε μια άλλη γραμμή.
4. Να αντιμεταθέσουμε δύο στήλες του πίνακα.
5. Να πολλαπλασιάσουμε μια στήλη του πίνακα με ένα μη μηδενικό στοιχείο του σώματος.

Οι παραπάνω πέντε μετασχηματισμοί λέγονται **στοιχειώδεις μετασχηματισμοί** του πίνακα .

Το επόμενο θεώρημα, το οποίο παραθέτουμε χωρίς απόδειξη, αποτελεί τη γνωστή (σχεδόν) σε όλους μας *Μέθοδο απαλοιφής του Gauss.*

Θεώρημα 2.1.14. *Κάθε $m \times n$ πίνακας* A *με στοιχεία από ένα σώμα* $\mathbb{F}$ *μπορεί να λάβει τη μορφή* $\left(\begin{array}{c|c} \mathrm{I}_r & \mathrm{B} \\ \hline 0 & 0 \end{array}\right)$ *εφαρμόζοντας μια πεπερασμένη ακολουθία στοιχειωδών μετασχηματισμών. Όπου r είναι η τάξη του πίνακα* A*, ο* B *είναι ένας $r \times (n-r)$ πίνακας και 0 μηδενικοί πίνακες αντίστοιχων διαστάσεων.*

Απόδειξη. Η ιδέα της απόδειξης είναι απλούστατη και μπορεί ο καθένας μας από μόνος του να τη συλλάβει. Άλλωστε σε όλα τα βιβλία Γραμμικής Άλγεβρας υπάρχει μια απόδειξη αντίστοιχου θεωρήματος.

□

Παρατήρηση 2.1.15. Ίσως αναρωτηθεί κάποιος γιατί στους στοιχειώδεις μετασχηματισμούς αναφέρεται ότι μπορούμε να προσθέσουμε ένα πολλαπλάσιο μιας γραμμής σε μια άλλη γραμμή, ενώ δεν αναφέρεται ότι μπορούμε να προσθέσουμε ένα πολλαπλάσιο μιας στήλης σε μια άλλη στήλη. Προσπαθήστε να δώσετε μια απάντηση.

2.1.2 Ασκήσεις

1. Έστω ο n-επαναληπτικός κώδικας $\mathcal{R}_p(n)$ $p-$αδικός κώδικας. Να υπολογίσετε έναν γεννήτορα πίνακά του.

2. Έστω $\mathcal{A}_n$ το σύνολο όλων των λέξεων του $\mathbb{Z}_2^n$ αρτίου βάρους. Δείξτε ότι το $\mathcal{A}_n$ είναι γραμμικός κώδικας. Υπολογίστε τις παραμέτρους του. Υπολογίστε μια βάση του και γράψτε έναν γεννήτορα πίνακα σε κανονική μορφή.

3. Έστω $\mathcal{E}_n$ το υποσύνολο του $\mathbb{F}_p^n$ που αποτελείται από όλες τις λέξεις $\mathbf{c} = c_1c_2\cdots c_n \in \mathbb{F}_p^n$ των οποίων το άθροισμα των χαρακτήρων ισούται με μηδέν, δηλαδή $\sum_{i=1}^n c_i = 0$. Στο Παράδειγμα $2.1.2_5$ είχαμε δεί ότι το $\mathcal{E}_n$ είναι ένας γραμμικός κώδικας. Να υπολογίσετε τις παραμέτρους του και έναν γεννήτορα πίνακα.

4. Δείξτε ότι σε έναν δυαδικό γραμμικό κώδικα $\mathcal{C}$ είτε όλες οι (κωδικο)λέξεις έχουν άρτιο βάρος είτε ακριβώς οι μίσες το πλήθος έχουν περιττό βάρος. Ισχύει κάτι ανάλογο σε τριαδικούς κώδικες;

5. Δείξτε ότι σε έναν γραμμικό κώδικα επί του σώματος $\mathbb{Z}_p$ είτε όλες οι (κωδικο)λέξεις αρχίζουν με 0, είτε ακριβώς $1/p$ το πλήθος αρχίζουν με μηδέν.

6. Έστω ένας $[n, k, d]$ γραμμικός κώδικας $\mathcal{C}$ επί του σώματος $\mathbb{Z}_p$. Δείξτε ότι το άθροισμα των βαρών όλων των στοιχείων του $\mathcal{C}$ είναι το πολύ ίσο με $n(p-1)p^{k-1}$.

7. Έστω ο $5-$αδικός γραμμικός κώδικας $\mathcal{C} \subseteq \mathbb{Z}_5^4$, ο οποίος παράγεται από το σύνολο $\{\, 0123,\, 0314,\, 0432 \,\}$. Να υπολογίσετε έναν γεννήτορα πίνακα σε κανονική μορφή και κατόπιν να υπολογίσετε τις παραμέτρους του.

8. Έστω $\mathcal{C}$, $\mathcal{D}$ δυαδικοί γραμμικοί κώδικες του ιδίου μήκους. Δείξτε ότι ο κώδικας που προκύπτει από μια $(\mathbf{u},\, \mathbf{u}+\mathbf{v})$- κατασκευή είναι επίσης γραμμικός. Υπολογίστε τις παραμέτρους του. Αν G, D είναι γεννήτορες πίνακες των $\mathcal{C}$ και $\mathcal{D}$ αντίστοιχα, να υπολογίσετε έναν γεννήτορα πίνακα του νέου κώδικα.

9. Έστω $\mathcal{C}_1$ και $\mathcal{C}_2$ γραμμικοί κώδικες επί του ιδίου σώματος με παραμέτρους $[n_1, k_1, d_1]$ και $[n_2, k_2, d_2]$ αντίστοιχα και γεννήτορες πίνακες G_1 και G_2 αντίστοιχα. Έστω $\mathcal{C}$ ο γραμμικός κώδικας με γεννήτορα πίνακα $\mathrm{G} = \begin{pmatrix} \mathbf{0} & \mathrm{G}_1 \\ \mathrm{G}_2 & * \end{pmatrix}$, όπου στη θέση του $*$ είναι ένας τυχαίος $k_2 \times n_1$ πίνακας με στοιχεία από το σώμα. Δείξτε ότι η ακτίνα κάλυψης του κώδικα $\mathcal{C}$ είναι μικρότερη ή ίση από το άθροισμα των ακτίνων κάλυψης των κωδίκων $\mathcal{C}_1$ και $\mathcal{C}_2$. Δηλαδή $cr(\mathcal{C}) \leq cr(\mathcal{C}_1) + cr(\mathcal{C}_2)$. (Για την ακτίνα κάλυψης δες τον Ορισμό 1.5.9).

2.2 Δυϊκοί κώδικες

Στα προηγούμενα είδαμε ότι η Γεωμετρική έννοια της απόστασης αποτελεί το βασικότερο συστατικό στην κατασκευή και στο χειρισμό ενός κώδικα. Εδώ θα δούμε πώς μια άλλη Γεωμετρική έννοια, η καθετότητα, αποβαίνει σημαντική για τους κώδικες και ιδιαίτερα για τους γραμμικούς κώδικες.

Θα ξεκινήσουμε με μερικούς γενικούς ορισμούς.

Ορισμός 2.2.1. *Έστω ένα σώμα* $\mathbb{F}$ *και* $\mathbf{x} = (x_1, x_2, \ldots, x_n)$, $\mathbf{y} = (y_1, y_2, \ldots, y_n) \in \mathbb{F}^n$, *όπου* n *είναι ένας φυσικός αριθμός. Το* **εσωτερικό γινόμενο** *των διανυσμάτων* $\mathbf{x} = (x_1, x_2, \ldots, x_n)$, $\mathbf{y} = (y_1, y_2, \ldots, y_n)$ *ορίζεται να είναι το στοιχείο* $< \mathbf{x}, \mathbf{y} > = x_1y_1 + x_2y_2 + \cdots + x_ny_n \in \mathbb{F}$

Παράδειγμα 2.2.2. Έστω $\mathbf{x} = (1, 2, 3), \mathbf{y} = (2, 3, 1) \in \mathbb{Z}_5^3$, τότε $< \mathbf{x}, \mathbf{y} > = \mathbf{x}\,\mathbf{y}^t = (1, 2, 3)\begin{pmatrix} 2 \\ 3 \\ 1 \end{pmatrix} = 1 \cdot 2 + 2 \cdot 3 + 3 \cdot 1 = 1$

Οι κυριώτερες ιδιότητες του εσωτερικού γινομένου συνοψίζονται στην επόμενη πρόταση.

Πρόταση 2.2.3. *Για κάθε* $\mathbf{x}, \mathbf{y}, \mathbf{z} \in \mathbb{F}^n$ *και κάθε* $\lambda \in \mathbb{F}$ *ισχύει.*

1. $< \mathbf{x}, \mathbf{y} > = < \mathbf{y}, \mathbf{x} >$.
2. $< (\mathbf{x} + \mathbf{y}), \mathbf{z} > = < \mathbf{x}, \mathbf{z} > + < \mathbf{y}, \mathbf{z} >$.
3. $< (\lambda\mathbf{x}), \mathbf{y} > = < \mathbf{x}, (\lambda\mathbf{y}) > = \lambda(< \mathbf{x}, \mathbf{y} >)$.

Απόδειξη. Άσκηση. □

Ορισμοί 2.2.4.
1. *Έστω* $\mathbf{x}, \mathbf{y} \in \mathbb{F}^n$. *Τα διανύσματα* $\mathbf{x}, \mathbf{y}$ *λέγονται* **κάθετα** *ή* **ορθογώνια** *αν* $< \mathbf{x}, \mathbf{y} > = < \mathbf{y}, \mathbf{x} > = \mathbf{0}$.
2. *Έστω* S *ένα μη κενό υποσύνολο του* $\mathbb{F}^n$, *τότε το σύνολο* $S^{\perp} = \{\, \mathbf{x} \in \mathbb{F}^n \mid < \mathbf{x}, \mathbf{s} > = 0$ *για όλα τα* $s \in S \,\}$ *ονομάζεται* **ορθογώνιο συμπλήρωμα** *του* S .

Παραδείγματα 2.2.5.
1. Έστω $\mathbf{x} = (1, 2, 3), \mathbf{y} = (2, 3, 4) \in \mathbb{Z}_5^3$, τότε $< \mathbf{x}, \mathbf{y} > = 0$, άρα τα $\mathbf{x}$ και $\mathbf{y}$ είναι κάθετα.
2. Έστω $\mathbf{x} = (1, 2, 3) \in \mathbb{Z}_7^3$, τότε $< \mathbf{x}, \mathbf{x} > = 0$, δηλαδή το $\mathbf{x} = (1, 2, 3)$ είναι κάθετο στον εαυτό του!
3. Έστω $S = \{\, (1, 1, \ldots, 1) \,\} \subseteq \mathbb{Z}_p^n$, τότε το ορθογώνιο συμπλήρωμα είναι ίσο με $S^{\perp} = \{\, (a_1, a_2, \ldots, a_n) \in \mathbb{Z}_p^n \mid \sum_{i=1}^{n} a_i = 0\}$.

   Στην ειδική περίπτωση, όπου $p = 2$, το ορθογώνιο συμπλήρωμα του S αποτελείται από όλες τις λέξεις αρτίου βάρους (γιατί;)

Παρατήρηση. Στο Παράδειγμα 2 παραπάνω, είδαμε ότι υπάρχουν μη μηδενικά διανύσματα τα οποία είναι κάθετα στον εαυτό τους, κάτι που δεν συμβαίνει αν βρισκόμαστε στο χώρο $\mathbb{R}^n$ με τη συνήθη γεωμετρική έννοια της καθετότητας.

Πρόταση 2.2.6. *Το ορθογώνιο συμπλήρωμα* $S^{\perp}$ *ενός υποσυνόλου* S *του διανυσματικού χώρου* $\mathbb{F}^n$ *είναι διανυσματικός υπόχωρος. Ισχύει δε* $S^{\perp} = (< S >)^{\perp}$, *όπου* $< S >$ *παριστά τον υπόχωρο τον παραγόμενο από το υποσύνολο* S.

Απόδειξη. Η απόδειξη είναι άμεση συνέπεια της Πρότασης 2.2.3 και αφήνεται ως άσκηση. □

Ορισμός 2.2.7. *Έστω $\mathcal{C} \subseteq \mathbb{A}^n$ ένας κώδικας. Το ορθογώνιο συμπλήρωμα $\mathcal{C}^\perp$ ονομάζεται* **δυϊκός** *κώδικας του κώδικα $\mathcal{C}$.*

Προφανώς, από την προηγούμενη πρόταση, ο δυϊκός κώδικας ενός κώδικα είναι γραμμικός κώδικας.

Πρόταση 2.2.8. *Έστω $\mathcal{C}_1, \mathcal{C}_2$ δύο κώδικες με $\mathcal{C}_1 \subseteq \mathcal{C}_2$. Τότε ισχύει $\mathcal{C}_2^\perp \subseteq \mathcal{C}_1^\perp$.*

Απόδειξη. Έστω $\mathbf{c} \in \mathcal{C}_2^\perp$. Η (κωδικο)λέξη $\mathbf{c}$ είναι κάθετη προς κάθε στοιχείο του κώδικα $\mathcal{C}_2$, άρα κάθε στοιχείο του $\mathcal{C}_1$ είναι κάθετο προς τη $\mathbf{c}$, αφού $\mathcal{C}_1, \mathcal{C}_2$. Δηλαδή η $\mathbf{c} \in \mathcal{C}_1^\perp$. □

Έστω $\mathcal{C} = \{ \mathbf{c_1}, \mathbf{c_2}, \ldots, \mathbf{c_m} \} \subseteq \mathbb{A}^n$ ένας κώδικας. Μπορούμε να περιγράψουμε τα στοιχεία του δυϊκού κώδικα $\mathcal{C}^\perp$ ως εξής: Για $\mathbf{x} = (x_1, x_2, \ldots, x_n) \in \mathcal{C}^\perp$, έχουμε $< \mathbf{x}, \mathbf{c_i} >= 0$ για $i = 1, 2, \ldots, m$. Επομένως, αν
$\mathbf{c_i} = (c_{i1}, c_{i2}, \ldots, c_{in})$, $i = 1, 2, \ldots, m$, οι προηγούμενες σχέσεις γίνονται:

$$\begin{aligned}
c_{11}x_1 + c_{12}x_2 + \cdots + c_{1n}x_n &= 0 \\
c_{21}x_1 + c_{22}x_2 + \cdots + c_{2n}x_n &= 0 \\
&\vdots \\
c_{i1}x_1 + c_{i2}x_2 + \cdots + c_{in}x_n &= 0 \\
&\vdots \\
c_{m1}x_1 + c_{m2}x_2 + \cdots + c_{mn}x_n &= 0.
\end{aligned}$$

Δηλαδή τα στοιχεία του δυϊκού κώδικα αποτελούν τη λύση ενός ομογενούς γραμμικού συστήματος.

Έστω ο πίνακας $\mathrm{P} = \begin{pmatrix} c_{11} & c_{12} & \cdots & c_{1n} \\ c_{21} & c_{22} & \cdots & c_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ c_{i1} & c_{i2} & \cdots & c_{in} \\ \vdots & \vdots & \vdots & \vdots \\ c_{m1} & c_{m2} & \cdots & c_{mn} \end{pmatrix}$.

Δηλαδή οι γραμμές του πίνακα P είναι οι (κωδικο)λέξεις του κώδικα $\mathcal{C}$.

Το προηγούμενο σύστημα θα μπορούσε να γραφεί υπό την μορφή
$(x_1, x_2, \cdots, x_n)\,\mathrm{P}^t = \mathbf{0}$.

Οι προηγούμενες εξισώσεις ονομάζονται **εξισώσεις ελέγχου ισοτιμίας** και ο πίνακας P ονομάζεται **πίνακας ελέγχου ισοτιμίας** για τον δυϊκό κώδικα $\mathcal{C}^\perp$.

Όπως είναι γνωστόν ο χώρος των λύσεων του προηγουμένου συστήματος έχει διάσταση ίση με $n - r$, όπου r είναι η τάξη $r(\mathrm{P})$ του πίνακα P. Δηλαδή ο δυϊκός κώδικας $\mathcal{C}^\perp$ είναι ένας γραμμικός κώδικας διάστασης $n - r$.

Παραδείγματα 2.2.9. 1. Έστω ο 5−δικός κώδικας $\mathcal{C} = \{\, 3013,\, 2004,\, 1012 \,\}$. Ο δυϊκός κώδικας είναι ίσος με $\mathcal{C}^{\perp} = \{\, \mathbf{x} = x_1x_2x_3x_4 \in \mathbb{Z}_5^4 \mid \mathbf{x}\mathrm{P}^t = \mathbf{0} \,\}$, όπου P είναι ο πίνακας ελέγχου ισοτιμίας και έχει ως γραμμές τα στοιχεία του κώδικα $\mathcal{C}$. Δηλαδή τα στοιχεία του $\mathcal{C}^{\perp}$ είναι η λύση του συστήματος

$$\begin{aligned} 3x_1 + 0x_2 + x_3 + 3x_4 &= 0 \\ 2x_1 + 0x_2 + 0x_3 + 4x_4 &= 0 \\ x_1 + 0x_2 + x_3 + 2x_4 &= 0. \end{aligned}$$

Ο πίνακας ελέγχου ισοτιμίας έχει τάξη ίση με 3 (γιατί;). Επομένως η διάσταση του δυϊκού κώδικα $\mathcal{C}^{\perp}$ είναι ίση με $4-3 = 1$, άρα ο $\mathcal{C}^{\perp}$ αποτελείται από 5^1 στοιχεία. (Θα μπορούσατε να τα υπολογίσετε; Θα μπορούσατε να υπολογίσετε μια βάση του;).

2. Έστω ο 2−δικός κώδικας $\mathcal{C} = \{\, 1011,\, 0001,\, 1010 \,\}$. Ο δυϊκός κώδικας είναι ίσος με $\mathcal{C}^{\perp} = \{\, \mathbf{x} =, x_1x_2x_3x_4 \in \mathbb{Z}_2^4 \mid \mathbf{x}\mathrm{P}^t = \mathbf{0} \,\}$, όπου P είναι ο πίνακας ελέγχου ισοτιμίας και έχει ως γραμμές τα στοιχεία του κώδικα $\mathcal{C}$. Δηλαδή τα στοιχεία του $\mathcal{C}^{\perp}$ είναι η λύση του συστήματος

$$\begin{aligned} 1x_1 + 0x_2 + x_3 + 1x_4 &= 0 \\ 0x_1 + 0x_2 + 0x_3 + x_4 &= 0 \\ x_1 + 0x_2 + x_3 + 0x_4 &= 0. \end{aligned}$$

Ο πίνακας ελέγχου ισοτιμίας έχει τάξη ίση με δύο (γιατί;). Επομένως η διάσταση του δυϊκού κώδικα $\mathcal{C}^{\perp}$ είναι ίση με $4-2 = 2$, άρα ο $\mathcal{C}^{\perp}$ αποτελείται από 2^2 στοιχεία. (Θα μπορούσατε να τα υπολογίσετε; Θα μπορούσατε να υπολογίσετε μια βάση του;).

Στο αμέσως προηγούμενο παράδειγμα οι γραμμές του πίνακα δεν είναι γραμμικώς ανεξάρτητες, συγκεκριμένα η δεύτερη γραμμή είναι το άθροισμα της πρώτης και τρίτης γραμμής. Επομένως για τον υπολογισμό των στοιχείων του δυϊκού κώδικα $\mathcal{C}^{\perp}$ θα μπορούσαμε να απαλείψουμε την δεύτερη γραμμή του αντίστοιχου ομογενούς συστήματος. Δηλαδή ο κώδικας $\mathcal{C}^{\perp}$ έχει και έναν *άλλο* πίνακα ελέγχου ισοτιμίας, τον $\bar{\mathrm{P}} = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix}$.

Η έννοια το πίνακα ελέγχου ισοτιμίας (και των εξισώσεων ελέγχου ισοτιμίας) έχει ορισθεί, προς το παρόν, για τον δυϊκό κώδικα $\mathcal{C}^{\perp}$ ενός (τυχαίου) κώδικα $\mathcal{C}$. Στα επόμενα θα δούμε ότι για **κάθε** γραμμικό κώδικα μπορεί να ορισθεί ένας πίνακας ελέγχου ισοτιμίας και θα διευκρινίσουμε τι σημαίνει ένας κώδικας έχει πολλούς πίνακες ελέγχου ισοτιμίας.

Ορισμός 2.2.10. *Έστω ένας κώδικας $\mathcal{C}$ μήκους n με στοιχεία από το αλφάβητο $\mathbb{A}$, αν υπάρχει $s \times n$ πίνακας P με την ιδιότητα $\mathcal{C} = \{\, \mathbf{c} \in \mathbb{A}^n \mid \mathbf{c}\mathrm{P}^t = \mathbf{0} \,\}$, τότε ο πίνακας P θα λέγεται πίνακας ελέγχου ισοτιμίας για τον κώδικα $\mathcal{C}$.*

Παρατήρηση 2.2.11. Αν υπάρχει πίνακας ισοτιμίας, έστω P, για τον κώδικα $\mathcal{C}$, τότε ο κώδικας είναι γραμμικός. Πράγματι, έστω $\mathbf{c}_1, \mathbf{c}_2 \in \mathcal{C}$, τότε $(\mathbf{c}_1 + \mathbf{c}_2)\mathrm{P} = \mathbf{c}_1\mathrm{P} + \mathbf{c}_2\mathrm{P} = \mathbf{0} + \mathbf{0} = \mathbf{0}$. Δηλαδή $\mathbf{c}_1 + \mathbf{c}_2 \in \mathcal{C}$. Επίσης για $\lambda \in \mathbb{A}$ και $\mathbf{c} \in \mathcal{C}$ έχουμε $(\lambda\mathbf{c})\mathrm{P} = \lambda(\mathbf{c}\mathrm{P}) = \lambda\mathbf{0} = \mathbf{0}$, επομένως $\lambda\mathbf{c} \in \mathcal{C}$, Άρα ο κώδικας $\mathcal{C}$ είναι γραμμικός.

Σημείωση: Θα μπορούσαμε να επιχειρηματολογίσουμε και ως εξής: Από τον τρόπο ορισμού του πίνακα ελέγχου ισοτιμίας προκύπτει ότι ο κώδικας είναι ο πυρήνας της γραμμικής απεικόνισης με πεδίο ορισμού τον διανυσματικό χώρο $\mathbb{A}^n$, η οποία ορίζεται από τον πίνακα P^t. Άρα ο κώδικας $\mathcal{C}$ είναι γραμμικός.

Πρόταση 2.2.12. *Έστω $\mathcal{C}$ ένας $[n, k, d]$ γραμμικός κώδικας και* G *ένας γεννήτορας πίνακας. Ένας $s \times n$ πίνακας* P *με στοιχεία από το αλφάβητο $\mathbb{A}$ του κώδικα και τάξη $r(\mathrm{P})$ ίση με $n - k$ είναι πίνακας ελέγχου ισοτιμίας του κώδικα $\mathcal{C}$ αν και μόνο αν $\mathrm{GP}^t = \mathbf{0}$.*

Απόδειξη. Ως γνωστόν ο κώδικας $\mathcal{C}$ είναι της μορφής

$\mathcal{C} = \{\, (\lambda_1, \lambda_2, \ldots, \lambda_k) \cdot \mathrm{G},\ (\lambda_1, \lambda_2, \ldots, \lambda_k) \in \mathbb{A}^k \,\}$. Επομένως για κάθε $\mathbf{c} \in \mathcal{C}$ υπάρχουν $\lambda_1, \lambda_2, \ldots, \lambda_k \in \mathbb{A}$ έτσι ώστε $\mathbf{c} = (\lambda_1, \lambda_2, \ldots, \lambda_k)\cdot\mathrm{G}$. Υποθέτουμε ότι $G\mathrm{P}^t = \mathbf{0}$, τότε για κάθε $\mathbf{c} \in \mathcal{C}$ έχουμε $\mathbf{c}\mathrm{P}^t = ((\lambda_1, \lambda_2, \ldots, \lambda_k) \cdot \mathrm{G}) \cdot \mathrm{P}^t = (\lambda_1, \lambda_2, \ldots, \lambda_k)\cdot(\mathrm{G}\cdot\mathrm{P}^t) = \mathbf{0}$. Δηλαδή $\mathcal{C} \subseteq \{\, \mathbf{x} \in \mathbb{A}^n \mid \mathbf{x}\mathrm{P}^t = \mathbf{0} \,\}$. Αλλά σύμφωνα με την προηγούμενη παρατήρηση το σύνολο $\{\, \mathbf{x} \in \mathbb{A}^n \mid \mathbf{x}\mathrm{P}^t = \mathbf{0} \,\}$ είναι ο πυρήνας της γραμμικής απεικόνισης με πεδίο ορισμού τον διανυσματικό χώρο $\mathbb{A}^n$, η οποία ορίζεται από τον πίνακα P^t, επομένως έχει διάσταση ίση με $n - r(\mathrm{P}^t) = n - r(\mathrm{P}) = n - (n - k) = k$. Οπότε από τη σχέση $\mathcal{C} \subseteq \{\, \mathbf{x} \in \mathbb{A}^n \mid \mathbf{x}\mathrm{P}^t = \mathbf{0} \,\}$ έχουμε ότι $\mathcal{C} = \{\, \mathbf{x} \in \mathbb{A}^n \mid \mathbf{x}\mathrm{P}^t = \mathbf{0} \,\}$. Επομένως, σύμφωνα με τον ορισμό του πίνακα ελέγχου ισοτιμίας, ο πίνακας P είναι πίνακας ελέγχου ισοτιμίας για τον κώδικα $\mathcal{C}$.

Αντίστροφα, υποθέτουμε ότι ο πίνακας P είναι πίνακας ελέγχου ισοτιμίας για τον κώδικα $\mathcal{C}$, τότε από τις σχέσεις

$\mathcal{C} = \{\, \mathbf{x} \in \mathbb{A}^n \mid \mathbf{x}\mathrm{P}^t = \mathbf{0} \,\}$

και $\mathcal{C} = \{\, (\lambda_1, \lambda_2, \ldots, \lambda_k) \cdot \mathrm{G},\ (\lambda_1, \lambda_2, \ldots, \lambda_k) \in \mathbb{A}^k \,\}$

έπεται ότι $G\mathrm{P}^t = \mathbf{0}$.

□

Θεώρημα 2.2.13. *Έστω $\mathcal{C}$ ένας $[n, k, d]$ γραμμικός κώδικας και G ένας γεννήτορας πίνακας.*

1. *Ο πίνακας G είναι πίνακας ελέγχου ισοτιμίας το δυϊκού γραμμικού κώδικα $\mathcal{C}^\perp$.*

2. *Ο δυϊκός κώδικας $\mathcal{C}^\perp$ έχει διάσταση ίση με $n - k$.*

3. $\mathcal{C} = (\mathcal{C}^{\perp})^{\perp}$.

4. *Έστω H ένας γεννήτορας πίνακας του δυϊκού κώδικα $\mathcal{C}^{\perp}$, ο H είναι πίνακας ελέγχου ισοτιμίας του γραμμικού κώδικα $\mathcal{C}$.*

Απόδειξη. 1. Έστω $\mathbf{u} \in \mathcal{C}^{\perp}$, τότε για κάθε $\mathbf{c} \in \mathcal{C}$ έχουμε $< \mathbf{c}, \mathbf{u} >= \mathbf{c}\mathbf{u}^t = 0$. Από τον ορισμό του γεννήτορα πίνακα έχουμε ότι
$\mathcal{C} = \{ (\lambda_1, \lambda_2, \ldots, \lambda_k) \cdot \mathrm{G} \mid (\lambda_1, \lambda_2, \ldots, \lambda_k) \in \mathbb{A}^k \}$.
Οπότε από την προηγούμενη σχέση έχουμε $((\lambda_1, \lambda_2, \ldots, \lambda_k) \cdot \mathrm{G})\mathbf{u}^t = 0$, για κάθε $(\lambda_1, \lambda_2, \ldots, \lambda_k) \in \mathbb{A}^k$, δηλαδή $(\lambda_1, \lambda_2, \ldots, \lambda_k) \cdot (\mathrm{G}\mathbf{u}^t) = 0$, για κάθε $(\lambda_1, \lambda_2, \ldots, \lambda_k) \in \mathbb{A}^k$. Αυτό σημαίνει ότι $\mathrm{G}\mathbf{u}^t = 0$, δηλαδή $\mathbf{u}\mathrm{G}^t = 0$, το οποίο αποδεικνύει ότι ο πίνακας G είναι πίνακας ελέγχου ισοτιμίας του δυϊκού κώδικα $\mathcal{C}^{\perp}$.

2. Έχουμε επισημάνει ότι ο δυϊκός κώδικας $\mathcal{C}^{\perp}$ έχει διάσταση ίση με $n - r$, όπου r είναι η τάξη $r(\mathrm{G})$ του πίνακα ελέγχου ισοτιμίας G. Αλλά ο πίνακας G, ως γεννήτορας πίνακας του κώδικα $\mathcal{C}$, έχει τάξη ίση με τη διάσταση του $\mathcal{C}$, άρα $r(\mathrm{G}) = k$. Δηλαδή ο δυϊκός κώδικας $\mathcal{C}^{\perp}$ έχει διάσταση ίση με $n - k$.

3. Από τον ορισμό του δυϊκού κώδικα έχουμε ότι $\mathcal{C} \subseteq (\mathcal{C}^{\perp})^{\perp}$. Από το 2. έχουμε ότι $\dim(\mathcal{C}^{\perp})^{\perp} = n - \dim \mathcal{C}^{\perp} = n - (n-k) = k = \dim \mathcal{C}$. Οπότε $\mathcal{C} = (\mathcal{C}^{\perp})^{\perp}$.

4. Από το 1. έχουμε ότι ο γεννήτορας πίνακας H του δυϊκού κώδικα $\mathcal{C}^{\perp}$ είναι πίνακας ελέγχου ισοτιμίας του κώδικα $(\mathcal{C}^{\perp})^{\perp} = \mathcal{C}$.

□

Πόρισμα 2.2.14. *1. Κάθε $s \times n$ πίνακας P με στοιχεία από ένα πεπερασμένο σώμα $\mathbb{F}$ είναι πίνακας ελέγχου ισοτιμίας ένος (μοναδικού) γραμμικού κώδικα $\mathcal{C} \subseteq \mathbb{F}^n$.*

2. *Κάθε $k \times n$ πίνακας A με στοιχεία από ένα πεπερασμένο σώμα $\mathbb{F}$ με τις γραμμές του γραμμικά ανεξάρτητες είναι γεννήτορας πίνακας ενός γραμμικού κώδικα $\mathcal{C} \subseteq \mathbb{F}^n$ και πίνακας ελέγχου ισοτιμίας του δυϊκού γραμμικού κώδικα $\mathcal{C}^{\perp} \subseteq \mathbb{F}^n$.*

3. *Κάθε γραμμικός κώδικας έχει (τουλάχιστον) ένα πίνακα ελέγχου ισοτιμίας.*

Απόδειξη. 1. Έστω $\mathcal{C} = \{ \mathbf{c} \in \mathbb{A}^n \mid \mathbf{c}\mathrm{P}^t = \mathbf{0} \}$ το σύνολο λύσεων του ομογενούς συστήματος $(x_1, x_2, \cdots, x_n)\,\mathrm{P}^t = \mathbf{0}$. Το σύνολο αυτό αποτελεί διανυσματικό υπόχωρο του $\mathbb{A}^n$, άρα ο $\mathcal{C}$ είναι γραμμικός.

2. Άμεσο από τα προηγούμενα.

3. Άμεσο από το 4. του προηγουμένου θεωρήματος.

□

Παρατηρήσεις 2.2.15. 1. Στο 1. του προηγουμένου πορίσματος ο κώδικας που ορίζεται είναι μοναδικός, ως ο χώρος των λύσεων ένος ομογενούς συστήματος. Επίσης δεν αναφέρεται τίποτε για την τάξη $r(\mathrm{P})$ του πίνακα. Απλώς να έχουμε υπ' όψιν ότι η διάσταση του κώδικα $\mathcal{C}$ είναι ίση με $n-r(\mathrm{P})$, (άρα στην ακραία περίπτωση, όπου $r(\mathrm{P}) = n$, ο πίνακας P είναι πίνακας ελέγχου ισοτιμίας του μηδενικού κώδικα).

2. Στο 3. του προηγουμένου πορίσματος αναφέρουμε ότι ένας κώδικας έχει τουλάχιστον ένα πίνακα ελέγχου ισοτιμίας. Επίσης στο τελευταίο παράδειγμα πριν τον ορισμο 2.2.10 είχαμε επισημάνει ότι ένας κώδικας μπορεί να έχει περισσότερους του ενός πίνακες ελέγχου ισοτιμίας. Πράγματι, για έναν γραμμικό κώδικα μήκους n (δηλαδή έναν διανυσματικό υπόχωρο του $\mathbb{A}^n$) μπορούμε να κατασκευάσουμε πολλά ομογενή γραμμικά συστήματα τα οποία να έχουν ως χώρο λύσεων τον δοθέντα κώδικα (γιατί;).

3. Προσοχή! ένας γεννήτορας πίνακας είναι πάντα ένας πίνακας ισοτιμίας ενός (του δυϊκού) κώδικα. Ένας πίνακας ελέγχου ισοτιμίας δεν είναι κατ' ανάγκη ένας γεννήτορας πίνακας ενός κώδικα.

Παραδείγματα 2.2.16. 1. Έστω ο πίνακας $\mathrm{G} = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix}$ με στοιχεία στο $\mathbb{Z}_2$. Ο G είναι γεννήτορας πίνακας του γραμμικού κώδικα $\mathcal{C} = \{\, 00000,\, 11100,\, 00011,\, 11111 \,\}$ (γιατί;) και πίνακας ελέγχου ισοτιμίας για το δυϊκό κώδικα $\mathcal{C}^{\perp} = \{\, \mathbf{x} = x_1x_2x_3x_4x_5 \in \mathbb{Z}_2^5 \mid \mathbf{x}\mathrm{G}^t = \mathbf{0} \,\} = \{\, 00000,\, 00011,\, 11000,\, 11011,\, 01100,\, 01111,\, 10100,\, 10111 \,\}$.

Ο πίνακας $\mathrm{H} = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \end{pmatrix}$ είναι γεννήτορας πίνακας του δυϊκού κώδικα $\mathcal{C}^{\perp}$ (γιατί;) και πίνακας ελέγχου ισοτιμίας για τον κώδικα $\mathcal{C}$.

2. Έστω $\mathrm{G} = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix}$ ο πίνακας του προηγουμένου παραδείγματος, αλλά τα στοιχεία του να θεωρούνται ως στοιχεία του $\mathbb{Z}_3$. Ο G είναι γεννήτορας πίνακας του γραμμικού κώδικα
$\mathcal{C} = \{\, 00000,\, 11100,\, 00011,\, 11111,\, 22200,\, 00022,\, 11122,\, 22211,\, 22222 \,\}$
(γιατί;) και πίνακας ελέγχου ισοτιμίας για το δυϊκό κώδικα

$\mathcal{C}^{\perp} = \{\, \mathbf{x} = x_1x_2x_3x_4x_5 \in \mathbb{Z}_3^5 \mid \mathbf{x}\mathrm{G}^t = \mathbf{0} \,\}$. Ο δυϊκός κώδικας έχει 27 το πλήθος στοιχεία (μπορείτε να τα υπολογίσετε;).

Ο πίνακας $\mathrm{H} = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 2 \\ 0 & 1 & 2 & 0 & 0 \end{pmatrix}$ είναι γεννήτορας πίνακας του δυϊκού κώδικα $\mathcal{C}^{\perp}$ (γιατί;) και πίνακας ελέγχου ισοτιμίας για τον κώδικα $\mathcal{C}$.

Στα προηγούμενα παραδείγματα για να υπολογίσουμε έναν πίνακα ελέγχου ισοτιμίας ενός γραμμικού κώδικα υπολογίζαμε έναν γεννήτορα πίνακα του αντίστοιχου δυϊκού κώδικα. Θα κλείσουμε την παράγραφο με μια αναφορά σε γραμμικούς κώδικες, οι οποίοι έχουν γεννήτορα πίνακα σε ανηγμένη κλιμακωτή μορφή και θα εξετάσουμε τους αντίστοιχους πίνακες ελέγχου ισοτιμίας.

Θεώρημα 2.2.17. *Ένας γραμμικός κώδικας $\mathcal{C}$ μήκους n έχει ως γεννήτορα πίνακα έναν πίνακα της μορφής $\mathrm{G} = [\mathrm{I}_k \,\mathrm{B}]$ αν και μόνο αν ο πίνακας $\mathrm{P} = [-\mathrm{B}^t \,\mathrm{I}_{n-k}]$ είναι ένας πίνακας ελέγχου ισοτιμίας για τον κώδικα $\mathcal{C}$.*

Απόδειξη. Ας υπολογίσουμε το γινόμενο της $i-$γραμμής του πίνακα G με την $j-$στήλη του πίνακα P^t (θεωρούμενες ως πίνακες).

$$(0 \cdots 1 \cdots 0\, b_{i1} \cdots b_{i,n-k}) \cdot \begin{pmatrix} -b_{1j} \\ \vdots \\ -b_{kj} \\ 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix} = -b_{ij} + b_{ij} = 0.$$

Επομένως έχουμε ότι $\mathrm{G} \cdot \mathrm{P}^t = \mathbf{0}$. Οπότε από την πρόταση 2.2.12 έπεται το αποτέλεσμα, καθότι η τάξη του πίνακα $\mathrm{P} = [-\mathrm{B}^t \,\mathrm{I}_{n-k}]$ είναι ίση με $n-k$.

□

Έχουμε δεί (2.1.12) ότι κάθε γραμμικός κώδικας $\mathcal{C}$ είναι ισοδύναμος με ένα γραμμικό κώδικα $\mathcal{D}$, ο οποίος έχει ένα γεννήτορα πίνακα της μορφής $\mathrm{G} = [\mathrm{I}_k \,\mathrm{B}]$. Στην περίπτωση αυτή ο υπολογισμός του πίνακα ελέγχου ισοτιμίας $\mathrm{P} = [-\mathrm{B}^t \,\mathrm{I}_{n-k}]$ είναι πλέον άμεσος.

Παράδειγμα 2.2.18. Έστω ο $3-$δικός γραμμικός κώδικας
$\mathcal{C} = \{\, 00000,\ 10022,\ 01022,\ 11011,\ 21000,\ 12000,\ 20011,\ 02011,\ 22022 \,\}$
(γιατί είναι γραμμικός;) Ένας γεννήτορας πίνακας είναι ο πίνακας

$\mathrm{G} = \begin{pmatrix} 1 & 0 & 0 & 2 & 2 \\ 0 & 1 & 0 & 2 & 2 \end{pmatrix}$. (Γιατί ο G είναι γεννήτορας πίνακας;). Οπότε ο πίνακας $\mathrm{P} = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{pmatrix}$ είναι πίνακας ελέγχου ισοτιμίας για τον κώδικα $\mathcal{C}$.

2.2.1 Κώδικες που προέρχονται από άλλους κώδικες (Η περίπτωση των γραμμικών κωδίκων)

Στην παράγραφο 1.4.1 είχαμε μελετήσει διαδικασίες πώς ένας κώδικας μπορεί να προέλθει από έναν άλλο κώδικα. Εδώ θα δούμε πώς μερικές από αυτές τις διαδικασίες εφαρμόζονται στη περίπτωση των γραμμικών κωδίκων.

Έστω ένας γραμμικός $[n,\, k,\, d]$ κώδικας $\mathcal{C}$ με γεννήτορα πίνακα έστω G. Αν επεκτείνουμε τον κώδικα $\mathcal{C}$ επισυνάπτοντας ένα ψηφίο ελέγχου ισοτιμίας, τότε ο κώδικας $\hat{\mathcal{C}}$ που προκύπτει είναι και αυτός γραμμικός (γιατί;). Ένας γεννήτορας πίνακας του $\hat{\mathcal{C}}$ μπορεί να προέλθει από τον γεννήτορα πίνακα G του κώδικα $\mathcal{C}$ επισυνάπτοντας ένα ψηφίο ελέγχου ισοτιμίας στις (κωδικο)λέξεις που αποτελούν τις γραμμές του G. Πράγματι, ο πίνακας, έστω $\hat{\mathrm{G}}$, που προκύπτει έχει k το πλήθος γραμμές, οι οποίες είναι γραμμικά ανεξάρτητες, αφού οι αντίστοιχες k το πλήθος γραμμές του πίνακα G είναι γραμμικά ανεξάρτητες. Επίσης αν $c_0\, c_1 \cdots c_n\, c_{n+1}$ είναι ένα στοιχείο του κώδικα $\hat{\mathcal{C}}$, τότε το $c_0\, c_1 \cdots c_n$ είναι ένα στοιχείο του κώδικα $\mathcal{C}$, άρα γραμμικός συνδυασμός των γραμμών του πίνακα G. Επιπλέον δε ισχύει $-c_{n+1} = c_0 + c_1 + \cdots + c_n$. Οπότε εύκολα διαπιστώνουμε (από τον τρόπο κατασκευής των γραμμών του πίνακα $\hat{\mathrm{G}}$) ότι το στοιχείο $c_0\, c_1 \cdots c_n\, c_{n+1}$ είναι γραμμικός συνδυασμός των γραμμών του $\hat{\mathrm{G}}$. Άρα ο κώδικας $\hat{\mathcal{C}}$ είναι ένας γραμμικός $[n+1,\, k,\, \hat{d}]$ κώδικας με ελάχιστη απόσταση $\hat{d}$ ίση με d ή $d+1$. Υπενθυμίζουμε δε ότι στην περίπτωση όπου ο κώδικας είναι δυαδικός, τότε η ελάχιστη απόσταση $\hat{d}$ είναι πάντα άρτια (βλέπε Πρόταση 1.4.8).

Έστω P ένας πίνακας ελέγχου ισοτιμίας του κώδικα $\mathcal{C}$, από την Πρόταση 2.2.12 έχουμε ότι $\mathrm{G}\cdot\mathrm{P}^{\mathrm{t}} = \mathbf{0}$. Επειδή για ένα στοιχείο $c_0\, c_1 \cdots c_n\, c_{n+1}$ του κώδικα $\hat{\mathcal{C}}$ ισχύει $c_0 + c_1 + \cdots + c_n = -c_{n+1}$, έπεται ότι ένας πίνακας ελέγχου ισοτιμίας του κώδικα $\hat{\mathcal{C}}$ είναι ο $(n-k+1)\times(n+1)$ πίνακας $\hat{\mathrm{P}} = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ & & \mathrm{P} & \mathbf{0} \end{pmatrix}$.

Έστω τώρα ένας γραμμικός $[n,\, k,\, d]$ κώδικας $\mathcal{C}$ με γεννήτορα πίνακα G και πίνακα ελέγχου ισοτιμίας P. Υποθέτουμε ότι θέλουμε να τον σμικρύνουμε διαγράφοντας ορισμένες (κωδικο)λέξεις, αλλά ο κώδικας που θα προκύψει να παραμείνει γραμμικός. Η διαδικασία είναι απλή, επειδή ο νέος κώδικας είναι υπόχωρος

του αρχικού, αρκεί από μια βάση του κώδικα $\mathcal{C}$ να εξαιρέσουμε μερικά στοιχεία και να πάρουμε τον (υπό)χωρο τον παραγόμενο από τα εναπομείναντα στοιχεία. Αυτό επιτυγχάνεται ως εξής: Οι γραμμές του γεννήτορα πίνακα αποτελούν μια βάση του $\mathcal{C}$, οπότε διαγράφοντας μερικές γραμμές προκύπτει ένας πίνακας G_1, ο οποίος είναι γεννήτορας ενός υποκώδικα $\mathcal{C}_1$ του κώδικα $\mathcal{C}$.

Θα μπορούσαμε να έχουμε το ίδιο αποτέλεσμα, αν αντί να διαγράψουμε μερικές γραμμές από τον γεννήτορα πίνακα, προσθέσουμε μερικές γραμμές στον πίνακα ελέγχου ισοτιμίας, **αλλά** αν θέλουμε ο κώδικας που θα προκύψει να είναι γνήσια μικρότερος από τον αρχικό, πρέπει η γραμμές που θα προσθέσουμε να είναι γραμμικά ανεξάρτητες από τις γραμμές του πίνακα ελέγχου ισοτιμίας του κώδικα $\mathcal{C}$ (βλέπε Πόρισμα 2.2.14).

Παράδειγμα 2.2.19. Έστω ένας δυαδικός γραμμικός κώδικας $\mathcal{C}$, ο οποίος περιέχει **και** λέξεις περιττού βάρους (λέξεις αρτίου βάρους περιέχει πάντα ένας γραμμικός κώδικας). Τότε μπορούμε να βρούμε μια βάση του, η οποία να περιέχει μόνο μια λέξη περιττού βάρους. Πράγματι, αρκεί να παρατηρήσουμε ότι το άθροισμα λέξεων περιττού βάρους είναι λέξη αρτίου βάρους. Οπότε αν $\{\mathbf{c_1}, \mathbf{c_2}, \ldots, \mathbf{c_i}, \ldots, \mathbf{c_k}\}$ είναι μια βάση του $\mathcal{C}$ με περισσότερα του ενός στοιχεία περιττού βάρους, τότε επιλέγοντας ένα από αυτά και προσθέτοντάς το σε όλα τα υπόλοιπα περιττού βάρους προκύπτει μια βάση με ένα μόνο στοιχείο περιττού βάρους.

Από τα προηγούμενα έπεται ότι υπάρχει ένας γεννήτορας πίνακας G του οποίου μια γραμμή να είναι περιττού βάρους, ενώ όλες οι υπόλοιπες να είναι αρτίου βάρους. Αν διαγράψουμε τη γραμμή περιττού βάρους προκύπτει ένας πίνακας G_1, ο οποίος είναι γεννήτορας ενός υποκώδικα $\mathcal{C}_1$, ο οποίος έχει διάσταση κατά ένα λιγότερο από τον αρχικό κώδικα $\mathcal{C}$ και ο οποίος περιέχει όλες τις (κωδικο)λέξεις αρτίου βάρους. (Σύγκρινε με την Άσκηση $2.1.2_4$).

Αν τώρα P είναι ένας πίνακας ελέγχου ισοτιμίας του κώδικα $\mathcal{C}$, τότε προσθέτοντας μια γραμμή της οποίας όλα τα στοιχεία είναι 1 προκύπτει ένας πίνακας P_1 ελέγχου ισοτιμίας για τον κώδικα $\mathcal{C}_1$.

Με την αντίστροφη διαδικασία μπορούμε να αυξήσουμε έναν γραμμικό κώδικα. Πράγματι, αν $\mathcal{C}$ είναι ένας γραμμικός κώδικας με γεννήτορα πίνακα G, τότε προσθέτοντας γραμμές στον γεννήτορα πίνακα, οι οποίες είναι γραμμικά ανεξάρτητες από τις υπόλοιπες, πέρνουμε έναν πίνακα, ο οποίος αποτελεί γεννήτορα πίνακα ενός γραμμικού κώδικα, έστω $\bar{\mathcal{C}}$, ο οποίος περιέχει τον $\mathcal{C}$.

Παρατήρηση 2.2.20. Αυξάνοντας/σμικρύνοντας έναν γραμμικό κώδικα, τότε ο δυϊκός κώδικας σμικρύνεται/αυξάνεται ανάλογα (βλέπε Θεώρημα 2.2.13).

2.2.2 Αυτοδυϊκοί κώδικες

Όπως είναι γνωστό από τη Γραμμική Άλγεβρα, όταν έχουμε ένα διανυσματικό χώρο επί του σώματος των πραγματικών αριθμών, τότε δεν υπάρχουν μη μηδενικά διανύσματα τα οποία να είναι κάθετα (ως προς το γνωστό εσωτερικό γινόμενο) προς τον εαυτό τους.

Στην περίπτωση όμως που έχουμε διανυσματικούς χώρους με συντελεστές από ένα πεπερασμένο σώμα τα πράγματα είναι διαφορετικά. Στο τελευταίο παράδειγμα παρατηρούμε ότι η (κωδικο)λέξη 10022 είναι κάθετη στον εαυτό της, όπως είχαμε επισημάνει κάτι ανάλογο και στο παράδειγμα 2.2.5(2).

Εδώ θα ασχοληθούμε με γραμμικούς κώδικας στους οποίους κάθε στοιχείο είναι κάθετο προς όλα τα στοιχεία του κώδικα και επιπλέον αν μια λέξη είναι κάθετη σε κάθε (κωδικο)λέξη, τότε αυτή η λέξη είναι αναγκαστικά στοιχείο του κώδικα.

Ορισμός 2.2.21. *Ένας γραμμικός κώδικας $\mathcal{C}$ λέγεται αυτοδυϊκός αν ισχύει $\mathcal{C} = \mathcal{C}^{\perp}$.*

Παράδειγμα 2.2.22. Προφανώς (γιατί;) ο δυαδικός γραμμικός κώδικας $\mathcal{C} = \{\, 0000,\, 1100,\, 0011,\, 1111 \,\}$ είναι αυτοδυϊκός.

Οι κυριώτερες ιδιότητες ενός αυτοδυϊκού κώδικα συνοψίζονται στο επόμενο θεώρημα.

Θεώρημα 2.2.23. *1. Έστω ένας αυτοδυϊκός γραμμικός κώδικας $\mathcal{C}$, τότε για κάθε δύο γεννήτορες πίνακες G και D του $\mathcal{C}$ ισχύει $\mathrm{G} \cdot \mathrm{D}^t = \mathbf{0}$.*

2. Ένας αυτοδυϊκός κώδικας $\mathcal{C}$ έχει άρτιο μήκος $n = 2k$ και διάσταση ίση με k.

Απόδειξη. 1. Ως γνωστόν οι γραμμές ενός γεννήτορα πίνακα ένος κώδικα αποτελούνται από τα διανύσματα μιας βάσης του κώδικα. Έστω $\mathrm{B} = \{\, \mathbf{b_1}, \mathbf{b_2}, \ldots, \mathbf{b_k}, \,\}$ και $\Delta = \{\, \mathbf{d_1}, \mathbf{d_2}, \ldots, \mathbf{d_k}, \,\}$ δύο βάσεις του κώδικα $\mathcal{C}$ έτσι ώστε οι αντίστοιχοι γεννήτορες πίνακες να είναι $\mathrm{G} = \begin{pmatrix} \mathbf{b_1} \\ \mathbf{b_2} \\ \vdots \\ \mathbf{b_k} \end{pmatrix}$ και

$$\mathrm{D} = \begin{pmatrix} \mathbf{d_1} \\ \mathbf{d_2} \\ \vdots \\ \mathbf{d_k} \end{pmatrix}.$$

Έχουμε υποθέσει ότι ο κώδικας είναι αυτοδυϊκός, τότε για $\mathbf{b_i} = (b_{i1}, b_{i2}, \ldots, b_{in}) \in \mathrm{B}$ και $\mathbf{d_j} = (d_{j1}, d_{j2}, \ldots, d_{jn}) \in \Delta$ έχουμε $< \mathbf{b_i}, \mathbf{d_j} >= b_{i1}d_{j1} + b_{i2}d_{j2} + \cdots + b_{in}d_{jn} = 0$. Αυτό ισχύει για όλα τα $i, j = 1, 2, \ldots, n$. Δηλαδή $\mathrm{G} \cdot \mathrm{D}^t = \mathbf{0}$.

2. Ως γνωστόν για τον δυϊκό κώδικα έχουμε $\dim(\mathcal{C}^\perp) = n - \dim(\mathcal{C})$, όπου n είναι το μήκος του κώδικα. Οπότε το αποτέλεσμα είναι άμεσο.

□

Παρατήρηση 2.2.24. Το αντίστροφο του 1. του προηγουμένου θεωρήματος δεν ισχύει. Για παράδειγμα ο δυαδικός κώδικας $\mathcal{C} = \{\, 0000, 1100 \,\}$ είναι γραμμικός έχει διάσταση 1 και ο (μοναδικός) γεννήτορας πίνακας είναι ο πίνακας γραμμή $\mathrm{G} = (1100)$. Προφανώς ισχύει $\mathrm{G}\mathrm{G}^\perp = 0$, αλλά ο κώδικας δεν είναι αυτοδυϊκός, αφού $< 1100, 0011 >= 0$ και $0011 \notin \mathcal{C}$.

Αν επιπλέον υποθέσουμε ότι ο κώδικας $\mathcal{C}$ έχει άρτιο μήκος $n = 2k$ και διάσταση ίση με k, τότε ισχύει το αντίστροφο.
Πράγματι, υποθέτουμε ότι $\mathrm{G} \cdot \mathrm{D}^t = \mathbf{0}$. Έστω $\mathbf{c}, \mathbf{d} \in \mathcal{C}$, εκφράζουμε το $\mathbf{c}$ ως γραμμικό συνδυασμό των στοιχείων της βάσης B και το $\mathbf{d}$ ως γραμμικό συνδυασμό των στοιχείων της βάσης Δ, δηλαδή υπάρχουν $\lambda_1, \lambda_2, \ldots, \lambda_k$ στο σώμα $\mathbb{A}$ έτσι ώστε $\mathbf{c} = \lambda_1\mathbf{b_1} + \lambda_2\mathbf{b_2} + \cdots + \lambda_k\mathbf{b_k}$ και $\mu_1, \mu_2, \ldots, \mu_k$ στο σώμα $\mathbb{A}$ έτσι ώστε $\mathbf{d} = \mu_1\mathbf{d_1} + \mu_2\mathbf{d_2} + \cdots + \mu_k\mathbf{d_k}$. Τότε από τις ιδιότητες που αναφέρονται στην Πρόταση 2.2.3 και από την υπόθεση ότι $\mathrm{G} \cdot \mathrm{D}^t = \mathbf{0}$ εύκολα έπεται ότι $< \mathbf{c}, \mathbf{d} >= 0$. Δηλαδή $\mathcal{C} \subseteq \mathcal{C}^\perp$, επειδή όμως $\dim(\mathcal{C}) = k = n - k = \dim(\mathcal{C}^\perp)$, το αποτέλεσμα έπεται.

Η επόμενη πρόταση μας δίνει μια ικανή συνθήκη για την ύπαρξη αυτοδυϊκών κωδίκων.

Πρόταση 2.2.25. *Έστω p πρώτος αριθμός της μορφής $p = 4r + 1$, τότε για κάθε άρτιο θετικό ακέραιο $n = 2k$ υπάρχει αυτοδυϊκός κώδικας επί του $\mathbb{Z}_p$ με μήκος n.*

Απόδειξη. Επειδή ο p είναι της μορφής $p = 4r + 1$, υπάρχουν θετικοί ακέραιοι a και b έτσι ώστε $p = a^2 + b^2$. Κατασκευάζουμε τις λέξεις μήκους n $\mathbf{e}_1 = a\,b\cdots o$, $\mathbf{e}_2 = 0\,0\,a\,b\cdots o$, $\ldots$, $\mathbf{e}_k = 0\,0\cdots a\,b$. Είναι εύκολο να ελέγξουμε ότι τα $\mathbf{e}_i$ είναι γραμμικά ανεξάρτητα και ότι ο κώδικας που παράγουν είναι αυτοδυϊκός.

□

Παρατηρήσεις 2.2.26. 1. Στην προηγούμενη πρόταση ισχυριστήκαμε ότι για τον $p = 4r+1$ υπάρχουν θετικοί ακέραιοι a και b έτσι ώστε $p = a^2+b^2$. Υπάρχει το εξής θεώρημα στη Θεωρία Αριθμών.

Ένας περιττός πρώτος p μπορεί να γραφεί ως άθροισμα δύο τετραγώνων ($p = a^2 + b^2$) αν και μόνο αν είναι της μορφής $p = 4r + 1$. Μάλιστα δε τα a και b είναι μοναδικά.

2. Υπάρχει και ένα άλλο θεώρημα στη Θεωρία Αριθμών.

   Ένας περιττός πρώτος p μπορεί να γραφεί ως άθροισμα τεσσάρων τετραγώνων.

   Οπότε μπορούμε να αποδείξουμε ότι αν p είναι ένας πρώτος της μορφής $p = 4r + 3$ και ο n είναι ένας θετικός ακέραιος της μορφής $n = 4m$, τότε υπάρχει αυτοδυϊκός κώδικας επί του $\mathbb{Z}_p$ με μήκος ίσον με n.

2.2.3 Υπολογισμός της ελάχιστης απόστασης σε ένα γραμμικό κώδικα

Πρόταση 2.2.27. *Έστω $\mathcal{C}$ ένας $[n, k, d]$ γραμμικός κώδικας με πίνακα ελέγχου ισοτιμίας P. Η ελάχιστη απόσταση d είναι ίση με τον μικρότερο αριθμό γραμμικών εξαρτημένων στηλών του P, (δηλαδή ο P έχει d το πλήθος γραμμικά εξαρτημένες στήλες και κάθε $d-1$ το πλήθος στήλες του είναι γραμμικά ανεξάτητες).*

Απόδειξη. Έστω $\mathbf{p_1}, \mathbf{p_2}, \ldots, \mathbf{p_n}$ οι στήλες του πίνακα P. Υποθέτουμε ότι από αυτές w το πλήθος είναι γραμμικά εξαρτημένες με το w το ελάχιστο δυνατόν. Τότε υπάρχουν συντελεστές $c_1, c_2, \ldots, c_n$ από το αλφάβητο $\mathbb{F}_p$ εκ των οποίων οι w το πλήθος είναι διάφοροι του μηδενός και οι υπόλοιποι είναι μηδέν έτσι ώστε $\mathbf{c_1 p_1} + c_2\mathbf{p_2} + \cdots + c_n\mathbf{p_n} = \mathbf{0}$.

Πράγματι, αν υποθέσουμε (άνευ βλάβης) ότι οι πρώτες $\mathbf{p_1}, \mathbf{p_2}, \ldots, \mathbf{p_w}$ στήλες είναι γραμμικά εξαρτημένες και δεν υπάρχει γνήσιο υποσύνολό τους που να είναι γραμμικά εξαρτημένο, τότε σε κάθε γραμμικό συνδυασμό τους $\lambda_\mathbf{1}\mathbf{p_1} + \lambda_2\mathbf{p_2} + \cdots + \lambda_w\mathbf{p_w} = \mathbf{0}$ όλοι οι συντελεστές πρέπει να είναι διάφοροι του μηδενός. Διαφορετικά, αν ένας ήταν μηδέν τότε θα υπήρχαν λιγότερα από w το πλήθος γραμμικά εξαρτημενες στήλες (γιατί;).

Επομένως βλέπουμε ότι $(c_1, c_2, \ldots, c_n) \cdot \mathrm{P}^t = \mathbf{0}$. Η τελευταία σχέση ισοδυναμεί με το ότι η λέξη $\mathbf{c} = c_1\, c_2 \ldots c_n$ ανήκει στο κώδικα $\mathcal{C}$. Δηλαδή έχουμε μια λέξη βάρους w, η οποία ανήκει στον κώδικα, οπότε από το θεώρημα 2.1.3 έχουμε ότι $d \leq w$. Επίσης αν $\mathbf{c}$ είναι μια (κωδικο)λέξη με βάρος ίσο με την ελάχιστη απόσταση του κώδικα, τότε για τον πίνακα P έχουμε $\mathbf{c}\mathrm{P}^t = \mathbf{0}$. Άρα d το πλήθος στήλες του πίνακα, που αντιστοιχούν στα μη μηδενικά στοιχειά της $\mathbf{c}$, είναι γραμμικά εξαρτημένες. Οπότε $w \leq d$ και το αποτέλεσμα έπεται.

□

Παράδειγμα 2.2.28. Θεωρούμε τον γραμμικό κώδικα $\mathcal{D}$ επί του $\mathbb{Z}_{11}$ με πίνακα ελέγχου ισοτιμίας τον $\mathrm{P} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \end{pmatrix}$. Ο κώδικας αυτός είναι ένας $[10, 8]$ κώδικας και θέλουμε να υπολογίσουμε την ελάχιστη απόστασή του. Επειδή σε κάθε στήλη του πίνακα το πρώτο στοιχείο είναι 1 προφανώς ανά δύο οι στήλες είναι γραμμικά ανεξάρτητες (γιατί;). Αλλά οι τρείς πρώτες στήλες είναι γραμμικά εξαρτημένες, καθότι έχουμε $\binom{1}{3} = 10\binom{1}{1} + 2\binom{1}{2}$ (οι πράξεις γίνονται στο $\mathbb{Z}_{11}$). Επομένως από την προηγούμενη πρόταση έχουμε ότι η ελάχιστη απόσταση του κώδικα $\mathcal{D}$ είναι ίση με τρία.

Παρατήρηση 2.2.29. Στη σελίδα 39 είχαμε ασχοληθεί με τον κώδικα $\mathcal{C} = \{\, \mathbf{c} = x_1x_2\cdots x_{10} \in \mathbb{Z}_{11}^{10} \mid x_{10} = x_1 + 2x_2 + 3x_3 + \cdots + 9x_9 \,\}$ και είχαμε επισημάνει ότι ο $\mathcal{C}$ είναι ένας διανυσματικός χώρος επί του σώματος $\mathbb{Z}_{11}$ με διάσταση 9 και ελάχιστη απόσταση ίση με 2. Δεν είναι δύσκολο να δούμε ότι ο κώδικας αυτός έχει ως πίνακα ελέγχου ισοτιμίας τον πίνακα $\mathrm{H} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \end{pmatrix}$ και ότι ο προηγούμενος κώδικας $\mathcal{D}$ προέρχεται από σμίκρυνση του κώδικα $\mathcal{C}$, αφού ο πίνακας ελέγχου ισοτιμίας του $\mathcal{D}$ προέρχεται από τον πίνακα ελέγχου ισοτιμίας του $\mathcal{C}$ με την επισύναψη μιας επιπλέον γραμμής.

Επίσης είχαμε δεί ότι ο κώδικας **ISBN** προέρχεται από σμίκρυνση του κώδικα $\mathcal{C}$. Εδώ είναι ευκαιρία να επισημάνουμε ότι ο κώδικας **ISBN δεν** είναι γραμμικός. Πράγματι, το διανύσμα $\mathbf{a} = 5\,5\,5\,5\,1\,1\;1\,1\,1\,8$ είναι μια (κωδικο)λέξη του κώδικα **ISBN**, αλλά $\mathbf{a} + \mathbf{a} = X\,X\,X\,X\,2\,2\;2\,2\,2\,5$ δεν ανήκει στον κώδικα **ISBN**.

Στην παράγραφο 1.5.2 είχαμε ασχοληθεί με το κάτω φράγμα Gilbert-Varshamov, εδώ θα δούμε ότι το φράγμα αυτό μπορεί να βελτιωθεί αν θεωρήσουμε γραμμικούς κώδικες.

Πρόταση 2.2.30. (Κάτω φράγμα των Gilbert-Varshamov για γραμμικούς κώδικες).

Υπάρχει ένας $p-$αδικός $[n, k]$ γραμμικός κώδικας με ελάχιστη απόσταση τουλάχιστον d, αρκεί να ισχύει

$$p^k < p^n / \sum_{i=0}^{d-2} \binom{n-1}{i} (p-1)^i \ .$$

Επομένως αν k είναι ο μεγαλύτερος ακέραιος που ικανοποιεί την παραπάνω ανισότητα, τότε $A_p(n, d) \geq p^k$.

Απόδειξη. Αν μπορέσουμε να κατασκευάσουμε έναν $(n-k) \times n$ πίνακα H με στοιχεία από το σώμα $\mathbb{F}_p$ έτσι ώστε κάθε σύνολο με $d-1$ το πλήθος από τις στήλες του να είναι γραμμικά ανεξάρτητο, τότε υπάρχει γραμμικός κώδικας με

πίνακα ελέγχου ισοτιμίας τον πίνακα αυτό (Πόρισμα 2.2.14). Σύμφωνα με την προηγούμενη πρόταση η ελάχιστη απόσταση αυτού του κώδικα θα είναι τουλάχιστον ίση με d και θα έχουμε τελειώσει.
Ως πρώτη στήλη μπορούμε να επιλέξουμε οποιαδήποτε μη μηδενική $(n-k)-$άδα. Ως δεύτερη στήλη επιλέγουμε οποιαδήποτε $(n-k)-$άδα αρκεί να μην είναι πολλαπλάσιο της πρώτης στήλης. Ως τρίτη στήλη επιλέγουμε οποιαδήποτε $(n-k)-$άδα αρκεί να μην είναι γραμμικός συνδυασμός των δύο προηγουμένων. Γενικά σκοπός μας είναι να επιλέξουμε την i στήλη έτσι ώστε να μην είναι γραμμικός συνδυασμός οποιωνδήποτε $d-2$ (ή λιγότερων) το πλήθος στηλών από τις $i-1$ το πλήθος στήλες που έχουν ήδη επιλεγεί. Δηλαδή αν έχουμε επιλέξει $i-1$ το πλήθος στήλες και πάρουμε τους γραμμικούς υπόχωρους του $\mathbb{F}_p^{n-k}$ διάστασης μικρότερης ή ίσης $d-2$ που παράγονται από στήλες που έχουν ήδη επιλεγεί, η $i-$οστή στήλη δεν πρέπει να βρίσκεται σε κανέναν από αυτούς τους υπόχωρους.

Έστω j $(j \leq d-2)$ το πλήθος στήλες από τις $i-1$ το πλήθος που έχουμε επιλέξει. Ας υπολογίσουμε το πλήθος των γραμμικών συνδυασμών (με μη μηδενικούς συντελεστές) που μπορούμε να σχηματίσουμε με αυτές τις στήλες. Υπάρχουν $(p-1)^j$ επιλογές μη μηδενικών συντελεστών, για κάθε μια από αυτές τις επιλογές έχουμε και έναν γραμμικό συνδυασμό. Τώρα τις j το πλήθος στήλες μπορούμε να τις επιλέξουμε με $\binom{i-1}{j}$ το πλήθος τρόπους. Άρα τελικά έχουμε $\binom{i-1}{j}(p-1)^j$ το πλήθος γραμμικούς συνδυασμούς j το πλήθος στηλών. Αθροίζοντας ως προς j έχουμε ότι το πλήθος των γραμμικών συνδυασμών από $d-2$ ή λιγότερες το πλήθος στήλες είναι ίσο με $N_i = \sum_{j=1}^{d-2}\binom{i-1}{j}(p-1)^j$.
Επομένως η i στήλη μπορεί να επιλεγεί από τα υπόλοιπα (μη μηδενικά) στοιχεία του διανυσματικού χώρου $\mathbb{F}_p^{n-k}$. Τα μη μηδενικά στοιχεία του $\mathbb{F}_p^{n-k}$ είναι $p^{n-k}-1$. Επομένως για να μπορούμε να επιλέξουμε την i στήλη πρέπει να ισχύει $N_i < p^{n-k}-1$. Τελικά για να μπορούμε να επιλέξουμε και την $n-$οστή στήλη πρέπει και αρκεί να ισχύει $N_n < p^{n-k}-1$, δηλαδή πρέπει και αρκεί να ισχύει $\sum_{j=1}^{d-2}\binom{n-1}{j}(p-1)^j < p^{n-k}-1$ ή ισοδύναμα $\sum_{j=0}^{d-2}\binom{n-1}{j}(p-1)^j < p^{n-k}$. Η τελευταία σχέση όμως ισχύει από την υπόθεση, επομένως έχουμε αποδείξει το ζητούμενο.

□

Παρατήρηση 2.2.31. Αν θελήσουμε να συγκρίνουμε το κάτω φράγμα Gilbert-Varshamov στη γενική του μορφή (Θεώρημα 1.5.17)με το κάτω φράγμα Gilbert-Varshamov για γραμμικούς κώδικες που επιτυνχάνεται στην προηγούμενη πρόταση, από το επόμενο παράδειγμα θα δούμε ότι το φράγμα Gilbert-Varshamov για γραμμικούς κώδικες είναι πολύ καλλίτερο. Θά πρέπει όμως να σημειωθεί ότι το πρώτο φράγμα αναφέρεται γενικά σε όλους τους κώδικες, ενώ το το δεύτερο αναφέρεται σε γραμμικούς κώδικες.

Παράδειγμα. Από το Θεώρημα 1.5.17 έχουμε ότι $A_2(5,\,3) \leq \frac{2^5}{1+\binom{5}{1}+\binom{5}{2}} = 2$.

Από την Πρόταση 2.2.30 έπεται ότι υπάρχει ένας δυαδικός $[5,\,k,\,3]$ γραμμικός κώδικας αρκεί να ισχύει $2^k < \frac{2^5}{1+\binom{4}{1}} = \frac{32}{5}$. Οπότε για $k = 2$ έχουμε ότι υπάρχει ένας δυαδικός $[5,\,2,\,3]$ γραμμικός κώδικας, επομένως $A_2(5,\,3) \leq 4$.

Αν ανατρέξουμε στον πίνακα 1.5.2 θα δούμε ότι $A_2(5,\,3) = 4$, δηλαδή το $A_2(5,\,3)$ λαμβάνει την κατώτερη (επιτρεπόμενη) τιμή.

2.2.4 Άσκήσεις

1. Έστω $A,\ B$ δύο υποσύνολα του $\mathbb{Z}_p^n$, με την ιδιότητα κάθε στοιχείο του A να είναι κάθετο με κάθε στοιχείο του B, δηλαδή $< \mathbf{a},\,\mathbf{b} >= 0$ για κάθε $\mathbf{a} \in A,\ \mathbf{b} \in B$. Υποθέτουμε ότι $\mid A \mid = p^k$ και $\mid B \mid \geq p^{n-k-1}+1$. Δείξτε ότι το A είναι ένας γραμμικός κώδικας. Υπολογίστε τον δυϊκό του.

2. Να υπολογίσετε έναν πίνακα ελέγχου ισοτιμίας για τον $n-$επαναληπτικό κώδικα $\mathcal{R}_p(n)$. Κατόπιν να περιγράψετε τον δυϊκό κώδικα $(\mathcal{R}_p(n))^{\perp}$ και να υπολογίσετε τις παραμέτρους του.

3. Δίνεται ο δυαδικός κώδικας $\mathcal{C}$ με πίνακα ελέγχου ισοτιμίας $\mathrm{P} = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}$ και ο τριαδικός κώδικας $\mathcal{D}$ με γεννήτορα πίνακα τον ίδιο πίνακα P. Να υπολογίσετε την ελάχιστη απόσταση του $\mathcal{C}$ και του $\mathcal{D}$.

4. Δείξτε ότι σε έναν δυαδικό αυτοδυϊκό κώδικα $\mathcal{C}$ όλες οι (κωδικο)λέξεις έχουν άρτιο βάρος, επιπλέον δείξτε ότι η λέξη $11\cdots 1 \in \mathcal{C}$. Ισχύει το αντίστροφο;

5. Δείξτε ότι για κάθε άρτιο θετικό ακέραιο n υπάρχει ένας δυαδικός αυτοδυϊκός κώδικας μήκους n.

6. Να κατασκευάσετε έναν δυαδικό αυτοδυϊκό κώδικα μήκους 8. Να υπολογίσετε την ελάχιστη απόστασή του.

7. Δείξτε ότι το βάρος κάθε (κωδικο)λέξης σε έναν τριαδικό αυτοδυϊκό κώδικα είναι πολλαπλάσιο του τρία.

8. Δείξτε ότι οι λέξεις 1201 και 1012 παράγουν έναν τριαδικό αυτοδυϊκό κώδικα. Βρείτε όλα τα στοιχεία του.

9. Υπάρχει αυτοδυϊκός κώδικας μήκους 6 επί του σώματος $\mathbb{Z}_7$;

10. Ένας γραμμικός κώδικας $\mathcal{C}$ λέγεται **αυτο-ορθογώνιος** αν ισχύει $\mathcal{C} \subseteq \mathcal{C}^{\perp}$.

    Δώστε ένα παράδειγμα ενός αυτο-ορθογώνιου κώδικα που δεν είναι αυτοδυϊκός.

    Έστω G ο γεννήτορας πίνακας ενός $p-$αδικού κώδικα $\mathcal{C}$ με $p = 2$ ή 3. Δείξτε ότι ο $\mathcal{C}$ είναι αυτο-ορθογώνιος αν και μόνο αν ανά δύο οι γραμμές του G είναι κάθετες και το βάρος κάθε γραμμής είναι πολλαπλάσιο του p.

11. Να υπολογίσετε το κάτω φράγμα Gilbert-Varshamov στις ακόλουθες περιπτώσεις: $A_2(6, 3)$, $A_2(7, 3)$, $A_2(8, 5)$. Συγκρίνετε τα αποτελέσματα με τις τιμές του πίνακα στη σελίδα 1.5.2.

2.3 Κωδικοποίηση και αποκωδικοποίηση με γραμμικούς κώδικες

Στην σελίδα 8 είχαμε αναφερθεί στη διαδικασία κωδικοποίησης - αποκωδικοποίησης. Συγκεκριμένα είχαμε ορίσει ως συνάρτηση κωδικοποίησης μια συνάρτηση $f : S \longrightarrow \mathcal{C}$ από το σύνολο πηγή S σε έναν κώδικα $\mathcal{C}$, η οποία είναι $1-1$ και επί.

Στην περίπτωση των γραμμικών κωδίκων η διαδικασία της κωδικοποίησης γίνεται ευκολότερη χρησιμοποιώντας τον γεννήτορα πίνακα του κώδικα.

Έτω $\mathcal{C}$ ένας $p-$αδικός $[n, k, d]$ γραμμικός κώδικας με γεννήτορα πίνακα τον $k \times n$ πίνακα G. Αν ως σύνολο πηγή επιλέξουμε τον διανυσματικό χώρο $\mathbb{F}_p^k$, τότε η συνάρτηση $f : \mathbb{F}_p^k \longrightarrow \mathcal{C}$ με $f(\mathbf{u}) = \mathbf{u}$G είναι μια συνάρτηση κωδικοποίησης αφού είναι 1-1 και επί (γιατί;). Επιπλέον η συνάρτηση f είναι γραμμική, επομένως μπορούμε να *εκμεταλευθούμε* όλες τις ιδιότητες των γραμμικών συνατρήσεων.

Στην περίπτωση, όπου ο γεννήτορας πίνακας είναι σε ανηγμένη κλιμακωτή μορφή $\mathrm{G} = [\mathrm{I}_k \, \mathrm{A}]$, έχουμε ότι η προς κωδικοποίηση λέξη $\mathbf{u} \in \mathbb{F}_p^k$ κωδικοιείται ως $\mathbf{u}[\mathrm{I}_k \, \mathrm{A}] = \mathbf{u}\,\mathbf{v}$, όπου $\mathbf{v} = \mathbf{u}$A, δηλαδή η κωδικοποιημένη λέξη αποτελείται από δύο τμήματα, το πρώτο είναι η προς κωδικοποίηση λέξη και το δεύτερο *πλεονάζον* τμήμα είναι το τμήμα που επισυνάπτεται για την προστασία από τους θορύβους κατά τη μετάδοση. (Μια ανάλογη συζήτηση έχει προηγηθεί στη σελίδα 63).

Η συνάρτηση αποκωδικοποίησης (βλέπε σελίδα 18) $\varphi : \mathbb{F}_p^n \longrightarrow \mathcal{C}$ ορίζεται από τον διανυσματικό χώρο $\mathbb{F}_p^n$ στον διανυσματικό υπόχωρο $\mathcal{C}$. Αυτό μας επιτρέπει να βρούμε *αποτελεσματικούς* τρόπους ανίχνευσης και διόρθωσης λάθών.

2.3.1 Διόρθωση λαθών με έναν γραμμικό κώδικα

Πριν δούμε πώς διορθώνουμε λάθη με έναν γραμμικό κώδικα εκμεταλευόμενοι το γεγονός ότι έχει τη δομή διανυσματικού χώρου, θα παραθέσουμε μερικά αποτε-

λέσματα απο τη Γραμμική Άλγεβρα.

Ορισμός 2.3.1. *Έστω V ένας διανυσματικός χώρος με συντελεστές από ένα (όχι κατ' ανάγκη πεπερασμένο) σώμα $\mathbb{F}$ και U ένας διανυσματικός υπόχωρος του V. Για κάθε $v \in V$ ορίζουμε το σύνολο $v + U = \{ v + u \mid u \in U \}$. Το σύνολο αυτό ονομάζεται* **σύμπλοκο** *του υπόχωρου U και το v* **αντιπρόσωπος** *του συμπλόκου .*

Θεώρημα 2.3.2. *Έστω V ένας διανυσματικός χώρος με συντελεστές από ένα σώμα $\mathbb{F}$, $a, b \in V$ και U ένας διανυσματικός υπόχωρος του V. Οι ακόλουθες προτάσεις είναι ισοδύναμες.*

1. $a + U = b + U$.
2. $a - b \in U$.
3. $b \in a + U$.

Απόδειξη. Έστω $x \in a + U = b + U$, τότε υπάρχουν $u_1, u_2 \in U$ έτσι ώστε $x = a + u_1 = b + u_2$, δηλαδή $a - b = u_2 - u_1$. Αλλά ο U είναι διανυσματικός υπόχωρος, επομένως $a - b = u_2 - u_1 \in U$. Δηλαδή $b = a + (u_1 - u_2) \in U$, οπότε για κάθε $u \in U$ έχουμε $b+u = a+(u_1-u_2)+u \in U$. Άρα $b+U \subseteq a+U$. Όμοια αποδεικνύεται ότι $a + U \subseteq b + U$.

□

Πόρισμα 2.3.3. *Με τις υποθέσεις του προηγουμένου θεωρήματος*

1. $a + U = U$ *αν και μόνο αν* $a \in U$.
2. *Δύο σύμπλοκα είτε συμπίπτουν είτε είναι ξένα μεταξύ τους. Δηλαδή αν* $(a + U) \cap (b + U) \neq \emptyset$, *τότε* $(a + U) = (b + U)$.
3. *Ένα στοιχείο του διανυσματικού χώρου V ανήκει σε (ακριβώς) ένα σύμπλοκο ως προς τον υπόχωρο U.*

Απόδειξη. 1. Προφανώς $a+U = U = 0+U$ αν και μόνο αν $a-0 = a \in U$.

2. Έστω $v \in (a + U) \cap (b + U)$, τότε $a + U = v + U = b + U$.

3. Κάθε $v \in V$ ανήκει σε ένα (ακριβώς) σύμπλοκο, το $v + U$.

□

Έστω τώρα ένας $[n, k, d]$ γραμμικός κώδικας $\mathcal{C}$ επί του αλφαβήτου $\mathbb{F}_p$. Το μέγεθος του $\mathcal{C}$ είναι ίσο με $M = p^k$ και για κάθε $\mathbf{x} \in \mathbb{F}_p^n$ το αντίστοιχο σύμπλοκο $\mathbf{x}+\mathcal{C}$ έχει τόσα στοιχεία όσα και ο κώδικας $\mathcal{C}$ (γιατί;). Επομένως υπάρχουν p^{n-k} το πλήθος διαφορετικά σύμπλοκα ως προς τον κώδικα (υπόχωρο) $\mathcal{C}$.

Έστω $\mathcal{C} = \{\mathbf{c}_1 = \mathbf{0}, \mathbf{c}_2, \mathbf{c}_3, \ldots, \mathbf{c}_M\}$. Επιλέγουμε έναν αντιπρόσωπο $\mathbf{a}_2 \in \mathbb{F}_p^n$ έτσι ώστε να μην ανήκει στον κώδικα $\mathcal{C}$ και να έχει μικρότερο βάρος από όλα τα στοιχεία του $\mathcal{C}$.
Το σύμπλοκο $\mathbf{a}_2+\mathcal{C} = \{\mathbf{a}_2+\mathbf{0}, \mathbf{a}_2+\mathbf{c}_2, \mathbf{a}_2+\mathbf{c}_3, \ldots, \mathbf{a}_2+\mathbf{c}_M\}$ είναι ξένο προς τον κώδικα. Κατόπιν επιλέγουμε έναν αντιπρόσωπο $\mathbf{a}_3 \in \mathbb{F}_p^n$ έτσι ώστε να μην ανήκει στην ένωση $\mathcal{C} \cup (\mathbf{a}_2+\mathcal{C})$ και να έχει μικρότερο βάρος από όλα τα στοιχεία του $\mathcal{C} \cup (\mathbf{a}_2+\mathcal{C})$. Συνεχίζοντας την ίδια διακασία επιλέγουμε έναν αντιπρόσωπο $\mathbf{a}_{i+1} \in \mathbb{F}_p^n$ έτσι ώστε να μην ανήκει στην ένωση $\mathcal{C} \cup (\mathbf{a}_2+\mathcal{C}) \cup (\mathbf{a}_3+\mathcal{C}) \cup \cdots \cup (\mathbf{a}_i+\mathcal{C})$ και να έχει μικρότερο βάρος από όλα τα στοιχεία του $\mathcal{C} \cup (\mathbf{a}_2+\mathcal{C}) \cup (\mathbf{a}_3+\mathcal{C}) \cup \cdots \cup (\mathbf{a}_i+\mathcal{C})$. Τελικά επιλέγουμε με την ίδια διαδικασία και τον τελευταίο αντιπρόσωπο $\mathbf{a}_r$, όπου $r = p^{n-k}$, οπότε το $\mathbb{F}_p^n$ γράφεται ως (διακεκριμένη) ένωση αυτών των συμπλόκων, δηλαδή $\mathbb{F}_p^n = \mathcal{C} \cup (\mathbf{a}_2 + \mathcal{C}) \cup (\mathbf{a}_3 + \mathcal{C}) \cup \cdots \cup (\mathbf{a}_r + \mathcal{C})$.

Σύμφωνα με την προηγούμενη διαδικασία τα στοιχεία του $\mathbb{F}_p^n$ θα μπορούσαν να *διευθετηθούν* σε έναν πίνακα

$\mathbf{0}$	$\mathbf{c}_2$	$\mathbf{c}_3$	$\cdots$	$\mathbf{c}_M$
$\mathbf{a}_2 + \mathbf{0}$	$\mathbf{a}_2 + \mathbf{c}_2$	$\mathbf{a}_2 + \mathbf{c}_3$	$\cdots$	$\mathbf{a}_2 + \mathbf{c}_M$
$\mathbf{a}_3 + \mathbf{0}$	$\mathbf{a}_3 + \mathbf{c}_2$	$\mathbf{a}_3 + \mathbf{c}_3$	$\cdots$	$\mathbf{a}_3 + \mathbf{c}_M$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$\mathbf{a}_r + \mathbf{0}$	$\mathbf{a}_r + \mathbf{c}_2$	$\mathbf{a}_r + \mathbf{c}_3$	$\cdots$	$\mathbf{a}_r + \mathbf{c}_M$

Ο πίνακας αυτός θα ονομάζεται **αντιπροσωπευτική διάταξη** των στοιχείων του $\mathbb{F}_p^n$ ως προς τους αντιπροσώπους $\mathbf{0}, \mathbf{a}_2, \mathbf{a}_3, \ldots, \mathbf{a}_r$.

Παρατηρήσεις 2.3.4.

Όπως βλέπουμε στον πίνακα, τα στοιχεία κάθε γραμμής (εκτός της πρώτης) είναι αθροίσματα των στοιχείων της πρώτης γραμμής με τον αντίστοιχο αντιπρόσωπο που βρίσκεται στην πρώτη στήλη. Δηλαδή, όταν μια (κωδικο)λέξη $\mathbf{c}$ διατρέχει τα στοιχεία του κώδικα $\mathcal{C}$, τότε τα στοιχείο $\mathbf{a}_i + \mathbf{c}$ διατρέχει τα στοιχεία της i γραμμής.

Μια αντιπροσωπευτική διάταξη **δεν** είναι μοναδική και εξαρτάται από την επιλογή των αντιπροσώπων. Η επιλογή αυτή έχει μεγάλη σημασία, όπως θα δούμε στα επόμενα, στην διόρθωση λαθών.

Παράδειγμα 2.3.5. Έστω ο δυαδικός κώδικας $\mathcal{C} = \{\, 0000,\ 1011,\ 0110,\ 1101 \,\}$. Μια αντιπροσωπευτική διάταξη των στοιχείων του $\mathbb{Z}_2^4$ είναι η εξής

0000	1011	0110	1101
1000	0011	1110	0101
0100	1111	0010	1001
0001	1010	0111	1100

Αν αντί του αντιπροσώπου 0100 επιλέξουμε τον αντιπρόσωπο 0010, τότε έχουμε την ακόλουθη αντιπροσωπευτική διάταξη

0000	1011	0110	1101
1000	0011	1110	0101
0010	1001	0100	1111
0001	1010	0111	1100

Έστω τώρα ένα στοιχείο $\mathbf{x} \in \mathbb{F}_p^n$, το στοιχείο αυτό καταλαμβάνει μια θέση, έστω $i\,j$, στον παραπάνω πίνακα, δηλαδή $\mathbf{x} = \mathbf{a}_i + \mathbf{c}_j$. Ας υπολογίσουμε την ελάχιστη απόσταση του $\mathbf{x}$ από τα στοιχεία του κώδικα $\mathcal{C}$. Ως γνωστόν ισχύει ότι $d(\mathbf{x},\, \mathbf{c}) = w(\mathbf{x} - \mathbf{c})$, επομένως
$\min\{\, d(\mathbf{x},\, \mathbf{c}),\ \mathbf{c} \in \mathcal{C} \,\} = \min\{\, w(\mathbf{x} - \mathbf{c}),\ \mathbf{c} \in \mathcal{C} \,\} =$
$= \min\{\, w((\mathbf{a}_i + \mathbf{c}_j) - \mathbf{c}),\ \mathbf{c} \in \mathcal{C} \,\} = \min\{\, w(\mathbf{a}_i + (\mathbf{c}_j - \mathbf{c})),\ \mathbf{c} \in \mathcal{C} \,\}$. Αλλά ο κώδικας $\mathcal{C}$ είναι διανυσματικός υπόχωρος, άρα όταν η (κωδικο)λέξη $\mathbf{c}$ διατρέχει τα στοιχεία του $\mathcal{C}$, τότε και η (κωδικο)λέξη $\mathbf{c}_j - \mathbf{c}$ διατρέχει όλα τα στοιχεία του $\mathcal{C}$. Επομένως συνεχίζοντας την προηγούμενη σχέση έχουμε
$\min\{\, w(\mathbf{a}_i + (\mathbf{c}_j - \mathbf{c})),\ \mathbf{c} \in \mathcal{C} \,\} = \min\{\, w(\mathbf{a}_i + \mathbf{c}),\ \mathbf{c} \in \mathcal{C} \,\} = w(\mathbf{a}_i) = w(\mathbf{x} - \mathbf{c}_j) = d(\mathbf{x},\, \mathbf{c}_j)$. Επομένως έχουμε ότι $\min\{\, d(\mathbf{x},\, \mathbf{c}),\ \mathbf{c} \in \mathcal{C} \,\} = d(\mathbf{x},\, \mathbf{c}_j)$. Δηλαδή βλέπουμε ότι η λέξη $\mathbf{x}$ που βρίσκεται στην j στήλη του πίνακα απέχει την μικρότερη απόσταση από την (κωδικο)λέξη που βρίσκεται στην κορυφή της αντίστοιχης στήλης. Όλα τα παραπάνω συνοψίζονται στο ακόλουθο Θεώρημα

Θεώρημα 2.3.6. *Έστω ένας $[n,\, k,\, d]$ κώδικας $\mathcal{C}$, μια αντιπροσωπευτική διάταξη των στοιχείων του $\mathbb{F}_p^n$ μπορεί να χρησιμεύσει για την αποκωδικοποίηση σύμφωνα με την αρχή της πλησιέστερης λέξης.*

Απόδειξη. Έστω ότι έχουμε επιλέξει μια αντιπροσωπευτική διάταξη των στοιχείων του $\mathbb{F}_p^n$ και ελήφθει η λέξη $\mathbf{x} \in \mathbb{F}_p^n$, έστω ότι αυτή η λέξη καταλαμβάνει την $i\,j$ θέση στον πίνακα, δηλαδή $\mathbf{x} = \mathbf{a}_i + \mathbf{c}_j$, ορίζουμε την συνάρτηση αποκωδικοποίησης ως εξής $\varphi : \mathbb{F}_p^n \longrightarrow \mathcal{C}$ με $\varphi(\mathbf{x}) = \mathbf{c}_j$.

□

Παρατηρήσεις 2.3.7. Η αποκωδικοποίση με τον τρόπο που περιγράψαμε πώς κατασκευάζεται μια αντιπροσωπευτική διάταξη είναι πάντα πλήρης (βλέπε Παρατήρηση 1.3.7). Αυτό **δεν** σημαίνει ότι πάντα η αποκωδικοποίηση είναι σωστή. Ενδέχεται να έχει σταλεί η (κωδικο)λέξη $\mathbf{c}_m$ και να έχει ληφθεί η λέξη $\mathbf{x}$, η οποία βρίσκεται στην $i\,j$ θέση στον πίνακα, δηλαδή $\mathbf{x} = \mathbf{a}_i + \mathbf{c}_j$, τότε αυτή θα αποκωδικοποιηθεί (λανθασμένα) ως $\mathbf{c}_j$ και **όχι** ως $\mathbf{c}_m$. Συγκεκριμένα μια λέξη $\mathbf{x}$ αποκωδικοποιείται σωστά αν και μόνο αν το διάνυσμα λάθους που (πιθανόν) παρέσφυσε είναι ένας από τους αντιπροσώπους που χρησιμοποίηθηκαν στη δημιουργία της αντιπροσωπευτικής διάταξης, δηλαδή αν $\mathbf{x} = \mathbf{a}_i + \mathbf{c}_j$, τότε η αποκωδικοποίηση είναι σωστή αν και μόνο αν ο *θόρυβος* που υπεισήλθε είναι το διανύσμα $\mathbf{a}_i$.

Παράδειγμα 2.3.8. Έστω ο κώδικας $\mathcal{C} = \{\,0000,\, 1011,\, 0110,\, 1101\,\}$ του προηγουμένου παραδείγματος. Υποθέτουμε ότι αποστέλλεται η λέξη 0110 και λαμβάνουμε τη λέξη 0100, η λέξη αυτή ισαπέχει από τις λέξεις του κώδικα 0000 και 0110 απόσταση ίση με ένα. Αν αρκεσθούμε γενικά στην αποκωδικοποίηση σύμφωνα με την αρχή της πλησιέστερης λέξης, τότε είμαστε αναγκασμένοι να δηλώσουμε *αμηχανία*. Αν χρησιμοποιήσουμε την αντιπροσωπευτική διάταξη που παριστάνεται στον πρώτο πίνακα, τότε αποκωδικοποιούμε λανθασμένα ως 0000. Αν όμως χρησιμοποιήσουμε την αντιπροσωπευτική διάταξη που παριστάνεται στον δεύτερο πίνακα, τότε αποκωδικοποιούμε σωστά ως 0110.

Παρατήρηση 2.3.9. Μπορείτε να αποδείξετε ότι η μόνη περίπτωση, όπου η αποκωδικοποίηση με τη βοήθεια μιας αντιπροσωπευτικής διάταξης ενδέχεται να είναι λανθασμένη, είναι όταν γενικά στην αποκωδικοποίηση σύμφωνα με την αρχή της πλησιέστερης λέξης είμαστε αναγκασμένοι να δηλώσουμε *αμηχανία*. Δηλαδή όταν σε μια γραμμή του πίνακα μιας αντιπροσωπευτικής διάταξης υπάρχουν δύο (τουλάχιστον) λέξεις με το ίδιο βάρος.

Δεδομένου ότι ένας κώδικας με ελάχιστη απόσταση ίση με d διορθώνει μέχρι $\lambda \leq \big[(d-1)/2\big]$ το πλήθος λάθη, σε έναν $[n,\, k,\, d]$ γραμμικό κώδικα όταν λαμβάνουμε μια αντιπροσωπευτική διάταξη των στοιχείων του $\mathbb{F}_p^n$ πρέπει (να φροντίζουμε) όλες οι λέξεις με βάρος το πολύ $\lambda = \big[(d-1)/2\big]$ να λαμβάνονται ως αντιπρόσωποι. Αυτό βεβαίως δεν σημαίνει ότι δεν υπάρχουν και άλλοι αντιπρόσωποι. Όπως συμβαίνει στην περίπτωση ένος τέλειου γραμμικού κώδικα, όπου όλοι οι αντιπρόσωποι είναι ακριβώς όλες οι λέξεις με βάρος μικρότερο ή ίσον με $\big[(d-1)/2\big]$ (γιατί;).

2.3.2 Η πιθανότητα σωστής αποκωδικοποίησης με έναν γραμμικό κώδικα

Έστω ένας $[n, k, d]$ γραμμικός κώδικας $\mathcal{C}$. Στην παράγραφο 1.3.1 είδαμε ότι η (δεσμευμένη) πιθανότητα $p(\mathbf{c} \mid \mathbf{c}) =$ η πιθανότητα σωστής αποκωδικοποίησης δεδομένου ότι εστάλει η λέξη $\mathbf{c}$ είναι ίση με το άθροισμα όλων των πιθανοτήτων $p(\,\textit{ελήφθει η λέξη}\ \mathbf{x} \mid \textit{εστάλει η λέξη}\ \mathbf{c}\,)$, όπου το $\mathbf{x}$ διατρέχει όλες τις λέξεις στο $\mathbb{F}_p^n$ που ικανοποιούν τη σχέση $\varphi(\mathbf{x}) = c$. Δηλαδή
$p(\mathbf{c} \mid \mathbf{c}) = \sum_{x \in \varphi^{-1}(\mathbf{c})} p(\,\textit{ελήφθει η λέξη}\ \mathbf{x} \mid \textit{εστάλει η λέξη}\ \mathbf{c}\,)$.

Έστω ότι για την αποκωδικοποίηση έχουμε επιλέξει μια αντιπροσωπευτική διάταξη με αντιπροσώπους $\mathbf{a}_1 = \mathbf{0}, \mathbf{a}_2, \mathbf{a}_3, \ldots, \mathbf{a}_r$, όπως είδαμε η συνάρτηση αποκωδικοποίησης ορίζεται για $\mathbf{x} = \mathbf{a}_i + \mathbf{c}_j$ ως $\varphi(\mathbf{a}_i + \mathbf{c}_j) = \mathbf{c}_j$. Επομένως έχουμε $p(\mathbf{c} \mid \mathbf{c}) = \sum_{i=1}^{r} p(\,\textit{παρέσφυσε το}\ \mathbf{a}_i\ \textit{ως λάθος}\,)$. Άρα το πρόβλημα ανάγεται στον υπολογισμό της πιθανότητας ένας από τους αντιπροσώπους που επιλέξαμε να παρεισφύσει ως διάνυσμα λάθους.

Για τον υπολογισμό της πιθανότητας $p(\,\textit{παρέσφυσε το}\ \mathbf{a}_i\ \textit{ως λάθος}\,)$ θα περιορισθούμε στην μερική περίπτωση ενός δυαδικού κώδικα, όπου η μετάδοση των μηνυμάτων γίνεται μέσω ενός αμνήμονος συμμετρικού διαύλου επικοινωνίας, όπου η πιθανότητα λανθασμένης μετάδοσης ενός χαρακτήρα είναι ίση με p. Έστω $w(\mathbf{a}_i)$ το βάρος του $\mathbf{a}_i$, το ότι ο $\mathbf{a}_i$ παρεισφύει ως λάθος στην (κωδικο)λέξη $\mathbf{c}_j$ που αποστέλλεται, σημαίνει ότι λαμβάνουμε τη λέξη $\mathbf{a}_i + \mathbf{c}_j$, επομένως *αλλοιώνονται* οι χαρακτήρες στις αντίστοιχες θέσεις που η λέξη $\mathbf{a}_i$ έχει 1. Άρα έχουμε $p(\,\textit{παρέσφυσε το}\ \mathbf{a}_i\ \textit{ως λάθος}\,) = p^{w(\mathbf{a}_i)}(1-p)^{n-w(\mathbf{a}_i)}$, οπότε αντικαθιστώντας στην προηγούμενη σχέση έχουμε $p(\mathbf{c} \mid \mathbf{c}) = \sum_{i=1}^{r} p^{w(\mathbf{a}_i)}(1-p)^{n-w(\mathbf{a}_i)}$.

Θα μπορούσαμε διαφορετικά να υπολογίσουμε την πιθανότητα σωστής αποκωδικοποίησης ως εξής· Έχουμε δεί (σελ. 16) ότι η πιθανότητα να *αλλοιωθούν* k το πλήθος χαρακτήρες είναι ίση με $p^k(1-p)^{n-k}$. Αν α_k παριστά το πλήθος των αντιπροσώπων με βάρος k, τότε προφανώς έχουμε $p(\mathbf{c} \mid \mathbf{c}) = \sum_{k=1}^{n} \alpha_k p^k (1-p)^{n-k}$. Επομένως έχουμε αποδείξει το επόμενο θεώρημα.

Θεώρημα 2.3.10. *Έστω $\mathcal{C}$ ένας $[n, k, d]$ δυαδικός γραμμικός κώδικας. Υποθέτουμε ότι έχουμε επιλέξει μια αντιπροσωπευτική διάταξη με αντιπροσώπους $\mathbf{a}_1 = \mathbf{0}, \mathbf{a}_2, \mathbf{a}_3, \ldots, \mathbf{a}_r$. Τότε η πιθανότητα σωστής αποκωδικοποίησης είναι ίση με*

$$p(\mathbf{c} \mid \mathbf{c}) = \sum_{i=1}^{r} p^{w(\mathbf{a}_i)}(1-p)^{n-w(\mathbf{a}_i)} = \sum_{k=1}^{n} \alpha_k p^k (1-p)^{n-k}\,.$$

Παράδειγμα 2.3.11. Έστω ο δυαδικός κώδικας $\mathcal{C} = \{\,0000, 1011, 0110, 1101\,\}$ του Παραδείγματος 2.3.5 με την ακόλουθη αντιπροσωπευτική διάταξη των στοιχείων του $\mathbb{Z}_2^4$.

0000	1011	0110	1101
1000	0011	1110	0101
0100	1111	0010	1001
0001	1010	0111	1100

Παρατηρούμε ότι $\alpha_0 = 1$, $\alpha_1 = 3$, $\alpha_2 = \alpha_3 = \alpha_4 = 0$, επομένως έχουμε $p(\mathbf{c} \mid \mathbf{c}) = (1-p)^4 + 3p(1-p)^3$. Αν, για παράδειγμα, έχουμε $p = 0.01$, τότε έχουμε $p(\mathbf{c} \mid \mathbf{c}) \approx 0.9897$. Επειδή το μέγεθος του κώδικα είναι τέσσερα, θα μπορούσαμε να υποθέσουμε ότι η πηγή είναι το σύνολο $\mathbb{Z}_2^2 = \{\,00,\, 01,\, 10,\, 11\,\}$ και τα στοιχεία της κωδικοποιούνται μεσω μιας συνάρτησης κωδικοποίησης $f : \mathbb{Z}_2^2 \longrightarrow \mathcal{C}$. Υποθέτουμε τώρα ότι το σύνολο $\mathbb{Z}_2^2$ (η πηγή) θεωρείται και κώδικας (στην πραγματικότητα εδώ η συνάρτηση κωδικοποίησης είναι η ταυτοτική συνάρτηση), οπότε (στην πραγματικότητα) το μήνυμα αποστέλλεται μη κωδικοποιημένο. Στην περίπτωση αυτή η πιθανότητα σωστής αποκωδικοποίησης είναι ίση με $p(\mathbf{c} \mid \mathbf{c}) = (1-p)^2 = 0.9801$ (γιατί;), η οποία είναι μικρότερη από την πιθανότητα σωστής αποκωδικοποίησης αν χρησιμοποιήσουμε τον κώδικα.

Εδώ θα θέλαμε να τονίσουμε, για άλλη μια φορά, το *κόστος* που επιφέρει η απαίτηση να αυξήσουμε την πιθανότητα σωστής αποκωδικοποίησης, καθότι την πρώτη φορά μεταδίδουμε λέξεις με τέσσερεις χαρακτήρες, ενώ τη δεύτερη λέξεις με δύο χαρακτήρες.

Ο προσδιορισμός, στο προηγούμενο θεώρημα, του πλήθους α_k των αντιπροσώπων βάρους k είναι πολύ δύσκολο να υπολογιστεί γενικά, μάλιστα υπάρχουν σημαντικές κατηγορίες κωδίκων, όπου τα αντίστοιχα α_k είναι άγνωστα. Στην περίπτωση όμως ενός τέλειου κώδικα τα α_k είναι εύκολο να υπλογισθούν. Πράγματι, στο τέλος της προηγουμένης παραγράφου είχαμε επισημάνει ότι στην περίπτωση ένος τέλειου γραμμικού κώδικα όλοι οι αντιπρόσωποι είναι ακριβώς όλες οι λέξεις με βάρος μικρότερο ή ίσον με $\big[(d-1)/2\big]$. Αλλά στο σύνολο $\mathbb{Z}_2^n$ υπάρχουν $\binom{n}{k}$ το πλήθος λέξεις βάρους k, επομένως έχουμε $\alpha_k = \binom{n}{k}$ για $0 \leq k \leq \big[(d-1)/2\big]$ και $\alpha_k = 0$ για $\big[(d-1)/2\big] \leq k \leq n$. Συνεπώς έχουμε.

Θεώρημα 2.3.12. *Σε έναν τέλειο $[n,\, k,\, d]$ δυαδικό γραμμικό κώδικα $\mathcal{C}$ η πιθανότητα σωστής αποκωδικοποίησης με μια αντιπροσωπευτική διάταξη είναι ίση με* $p(\mathbf{c} \mid \mathbf{c}) = \sum_{k=0}^{t} \binom{n}{k} p^k (1-p)^{n-k}$.

2.3.3 Ανίχνευση λαθών με έναν γραμμικό κώδικα

Υποθέτουμε ότι έχουμε έναν γραμμικό κώδικα $\mathcal{C}$ $[n,\, k,\, d]$, τον οποίο χρησιμοποιούμε (μόνο) για ανίχνευση λαθών.

Έστω ότι εστάλει η (κωδικο)λέξη $\mathbf{a}$, αλλά ελήφθει η λέξη $\mathbf{x}$. Αν υπεισήλθε λάθος, αυτό θα διαφύγει της προσοχής μας αν και μόνο αν η $\mathbf{x} \in \mathcal{C}$. Ο κώδικας

όμως είναι γραμμικός. Άρα το λάθος $\mathbf{e} = \mathbf{x} - \mathbf{a}$ δεν ανιχνεύται αν και μόνο αν $\mathbf{e} \in \mathcal{C}$.

Αν θέλουμε να υπολογίσουμε την πιθανότητα **μη** ανίχνευσης λαθών θα πρέπει να υπολογίσουμε την πιθανότητα σε κάθε (κωδικο)λέξη να επέλθουν τόσες αλλοιώσεις έτσι ώστε να προκύψει μια άλλη (κωδικο)λέξη και μετά να αθροίσουμε. Στην μερική περίπτωση ενός δυαδικού κώδικα, όπου η μετάδοση των μηνυμάτων γίνεται μέσω ενός αμνήμονος συμμετρικού διαύλου επικοινωνίας, όπου η πιθανότητα λανθασμένης μετάδοσης ενός χαρακτήρα είναι ίση με p έχουμε το επόμενο θεώρημα.

Θεώρημα 2.3.13. *Έστω $\mathcal{C}$ $[n, k, d]$ ένας δυαδικός γραμμικός κώδικας. Με A_i συμβολίζουμε το πλήθος των στοιχείων του $\mathcal{C}$ που έχουν βάρος ίσο με i. Η πιθανότητα $p($ μη ανίχνευσης λαθών $)$ εξαρτάται μόνο από τον κώδικα και τον δίαυλο επικοινωνίας και είναι ίση με $p($ μη ανίχνευσης λαθών $) = \sum_{i=1}^{n} A_i \cdot p^i \cdot (1-p)^{n-i}$.*

Απόδειξη. Όπως γνωρίζουμε (βλέπε σελίδα 16) η πιθανότητα να *αλλοιωθούν* i το πλήθος χαρακτήρες είναι ίση με $p^i(1-p)^{n-i}$. Προηγουμένως είδαμε ότι ένα λάθος δεν ανιχνεύεται αν και μόνο αν είναι στοιχείο του κώδικα $\mathcal{C}$. Θεωρούμε ότι κάθε μη μηδενική (κωδικο)λέξη βάρους i προέρχεται από αλλοίωση i το πλήθος χαρακτήρων της μηδενικής λέξης. Επομένως εύκολα έπεται το αποτέλεσμα.

□

Παράδειγμα 2.3.14. Έστω ο δυαδικός κώδικας $\mathcal{C} = \{\, 0000,\ 1011,\ 0110,\ 1101 \,\}$ του Παραδείγματος 2.3.11. Παρατηρούμε ότι $A_1 = 0$, $A_2 = 1$, $A_3 = 2$, $A_4 = 0$, επομένως έχουμε $p($ *μη ανίχνευσης λαθών* $) = \sum_{i=1}^{4} A_i \cdot p^i \cdot (1-p)^{n-i} = p^2(1-p)^2 + 2p^3(1-p) = p^2 - p^4$. Αν, για παράδειγμα, έχουμε $p = 0.01$, τότε έχουμε $p($ *μη ανίχνευσης λαθών* $) = 0.00009999$.

Παρατηρήσεις 2.3.15.

1. Αν συγκρίνουμε τα αποτελέσματα στα δύο Παραδείγματα 2.3.5 και 2.3.11, βλέπουμε ότι η πιθανότητα μη σωστής αποκωδικοποίησης είναι ίση με $1 - p(\mathbf{c} \mid \mathbf{c}) \approx 1 - 0.9897 = 0,0103$, ενώ η πιθανότητα $p($ *μη ανίχνευσης λαθών* $) = 0.00009999$. Αυτό είναι αναμενόμενο, διότι αν εφαρμόσουμε την αρχή αποκωδικοποίησης ως προς τη πλησιέστερη λέξη τότε ενδέχεται μια ληφθείσα λέξη να αποκωδικοποιθεί λανθασμένα.

2. Στο προηγούμενο άθροισμα $\sum_{i=1}^{n} A_i \cdot p^i \cdot (1-p)^{n-i}$ οι παράγοντες A_i είναι δύσκολο να υπολογισθούν στη γενική περίπτωση. Το πρόβλημα υπολογισμού των A_i παρουσιάζει μεγάλο θεωρητικό και πρακτικό ενδιαφέρον. Μια πρώτη προσέγγιση θα επιχειρήσουμε στην Παράγραφο 2.4

2.3.4 Το σύνδρομο σε έναν γραμμικό κώδικα

Η αποκωδικοποίηση με τη βοήθεια μιας αντιπροσωπευτικής διάταξης παρουσιάζει εγγενείς δυσκολίες, καθότι (ιδίως όταν το μήκος n του κώδικα είναι μεγάλο) χρειάζεται αρκετός χρόνος να εντοπιστεί η θέση μιας λέξης που λαμβάνεται, ούτως ώστε να αποκωδικοποιηθεί ως η λέξη που βρίσκεται στην κορυφή της στήλης στην οποία βρίσκεται. Όπως θα δούμε μπορούμε να συντομεύσουμε δραστικά την παραπάνω διαδικασία.

Έστω $\mathcal{C}$ ένας $[n, k, d]$ γραμμικός κώδικας και P ένας $s \times n$ πίνακας ελέγχου ισοτιμίας του $\mathcal{C}$. Για $\mathbf{x} \in \mathbb{F}_p^n$ το στοιχείο $\mathbf{x}\mathrm{P}^t$ θα λέγεται το **σύνδρομο** του $\mathbf{x}$.

Ως γνωστόν ο πίνακας P^t ορίζει μια γραμμική απεικόνιση $h : \mathbb{F}_p^n \longrightarrow \mathbb{F}_p^s$ με $h(\mathbf{x}) = \mathbf{x}\mathrm{P}^t$, δηλαδή το σύνδρομο του $\mathbf{x}$ είναι η εικόνα του μέσω της γραμμικής απεικόνισης h.

Από τον ορισμό του πίνακα ελέγχου ισοτιμίας (Ορισμός 2.2.10) για τον κώδικα $\mathcal{C}$ έχουμε $\mathcal{C} = \{\, \mathbf{c} \in \mathbb{A}^n \mid \mathbf{c}\mathrm{P}^t = \mathbf{0} \,\}$, δηλαδή ο κώδικας είναι ο πυρήνας της γραμμικής απεικόνισης h.

Πρόταση 2.3.16. *Έστω $\mathcal{C}$ ένας $[n, k, d]$ γραμμικός κώδικας και P ένας $s \times n$ πίνακας ελέγχου ισοτιμίας του. Δύο στοιχεία του $\mathbf{x}, \mathbf{y} \in \mathbb{F}_p^n$ έχουν το ίδιο σύνδρομο αν και μόνο αν τα αντίστοιχα σύμπλοκα ως προς τον $\mathcal{C}$ είναι ίσα.*

Απόδειξη. Η απόδειξη είναι άμεση καθότι η απεικόνιση h είναι γραμμική και ο πυρήνας της αποτελείται από τα στοιχεία του κώδικα $\mathcal{C}$.

Διαφορετικά θα μπορούσαμε να πούμε ότι $\mathbf{x} + \mathcal{C} = \mathbf{y} + \mathcal{C}$ αν και μόνο αν (από το Θεώρημα 2.3.2) $\mathbf{x} - \mathbf{y} \in \mathcal{C}$, αν και μόνο αν $(\mathbf{x} - \mathbf{y})\mathrm{P}^t = \mathbf{0}$ (από τον ορισμό του πίνακα ελεγχου ισοτιμίας), αν και μόνο αν $\mathbf{x}\mathrm{P}^t = \mathbf{y}\mathrm{P}^t$.

□

Από την προηγούμενη πρόταση βλέπουμε ότι υπάρχει μια ένα προς ένα και επί αντιστοιχία μεταξύ των συμπλόκων του κώδικα και των συνδρόμων.

Έστω τώρα μια αντιπροσωπευτική διάταξη των στοιχείων του $\mathbb{F}_p^n$ ως προς τους αντιπροσώπους $\mathbf{0}, \mathbf{a}_2, \mathbf{a}_3, \ldots, \mathbf{a}_r$. Υποθέτουμε ότι ελήφθει η λέξη $\mathbf{x}$, η οποία καταλαμβάνει μια θέση, έστω $i\,j$, στον πίνακα της αντιπροσωπευτικής διάταξης, δηλαδή $\mathbf{x} = \mathbf{a}_i + \mathbf{c}_j$. Σύμφωνα με τα προηγούμενα η λέξη θα αποκωδικοποιηθεί ως η (κωδικο)λέξη $\mathbf{c}_j = \mathbf{x} - \mathbf{a}_i$. Επομένως το πρόβλημα είναι να εντοπιστεί ο αντιπρόσωπος $\mathbf{a}_i$. Από την προηγούμενη πρόταση όμως έχουμε ότι η λέξη $\mathbf{x}$ και ο αντιπρόσωπος $\mathbf{a}_i$ έχουν το ίδιο σύνδρομο. Επομένως, αν γνωρίζουμε τα σύνδρομα των αντιπροσώπων, μπορούμε εύκολα να προχωρήσουμε στην αποκωδικοποίηση σύμφωνα με τον ακόλουθο αλγόριθμο.

Επισυνάπτουμε (προσωρινά) στην αντιπροσωπευτική διάταξη μια επιπλέον στήλη υπολογίζοντας τα σύνδρομα των αντιπροσώπων. Όταν λαμβάνουμε μια

λέξη υπολογίζουμε το σύνδρομό της και το συγκρίνουμε με τα σύνδρομα των αντιπροσώπων, με αυτό τον τρόπο εντοπίζουμε τον αντίστοιχο αντιπρόσωπο και αποκωδικοποιούμε αφαιρώντας από τη λέξη που λάβαμε τον αντιπρόσωπο που εντοπίσαμε.

Όπως βλέπουμε για την αποκωδικοποίηση πλέον **δεν** χρειαζόμαστε όλη την αντιπροσωπευτική διάταξη, αλλά μόνο δύο στήλες, την στήλη των αντιπροσώπων και την στήλη των αντίστοιχων συνδρόμων.

Παραδείγματα 2.3.17. 1. Έστω ο δυαδικός κώδικας $\mathcal{C} = \{\,0000,\, 1011,\, 0110,\, 1101\,\}$ του Παραδείγματος 2.3.5 με την αντιπροσωπευτική διάταξη των στοιχείων του $\mathbb{Z}_2^4$

0000	1011	0110	1101
1000	0011	1110	0101
0100	1111	0010	1001
0001	1010	0111	1100

Ένας πίνακας ελέγχου ισοτιμίας είναι ο $\mathrm{P} = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}$ (γιατί;)

Υπολογίζουμε τα σύνδρομα των αντιπροσώπων (δηλαδή τα σύνδρομα των στοιχείων της πρώτης στήλης).
$(0\,0\,0\,0)\mathrm{P}^t = (0\,0),\ (1\,0\,0\,0)\mathrm{P}^t = (1,\,1),\ (0,\,1,\,0,\,0)\mathrm{P}^t = (1,\,0),$
$(0,\,0,\,0,\,1)\mathrm{P}^t = (0,\,1).$
Υποθέτουμε ότι λαμβάνουμε τη λέξη $0\,1\,1\,1$, αν θέλαμε να χρησιμοποιήσουμε την παραπάνω αντιπροσωπευτική διάταξη θα έπρεπε να εντοπίσουμε τη θέση της και κατά τα γνωστά να την αποκωδικοποιήσουμε. Τώρα υπολογίζουμε το σύνδρομό της $(0\,1\,1\,1)\mathrm{P}^t = (0\,1)$, βλέπουμε ότι είναι το ίδιο με το σύνδρομο του αντιπροσώπου $0\,0\,0\,1$. Επομένως σύμφωνα με τον προηγούμενο αλγόριθμο αποκωδικοποιούμε ως $0\,1\,1\,1 - 0\,0\,0\,1 = 0\,1\,1\,0 \in \mathcal{C}$. Δηλαδή για την αποκωδικοποίηση αντί του προηγουμένου πίνακα είναι αρκετός ο πίνακας

0000	00
1000	11
0100	10
0001	01

ο οποίος έχει μόνο δύο στήλες .

2. Θεωρούμε τον γραμμικό κώδικα $\mathcal{D}$ επί του $\mathbb{Z}_{11}$ με πίνακα ελέγχου ισοτιμίας

τον $\mathrm{P} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \end{pmatrix}$. Ο κώδικας αυτός είναι ένας $[10, 8]$ κώδικας και στο Παράδειγμα 2.2.28 είχαμε υπολογίσει ότι η ελάχιστη απόστασή του είναι ίση με τρία. Επομένως διορθώνει ένα λάθος. Θα δούμε ότι ο κώδικας αυτός έχει την επιπλέον ιδιότητα. Ταυτόχρονα με την διόρθωση ενός λάθους μπορεί να ανιχνεύει την ύπαρξη δύο λαθών, τα οποία προέρχονται από την αντιμετάθεση δύο χαρακτήρων κατά τη μετάδοση μιας (κωδικο)λέξης.

Έστω ότι εστάλει η (κωδικο)λέξη $\mathbf{a} = a_1\, a_2 \cdots a_{10}$, αλλά ελήφθει η λέξη $\mathbf{x} = x_1\, x_2 \cdots x_{10}$, στην οποία σε μια θέση υπεισήλθε ένα λάθος. Δηλαδή $\mathbf{x} = x_1\, x_2 \cdots x_{10} = a_1\, a_2 \cdots a_j + k, \cdots a_{10}$.

Υπολογίζουμε το σύνδρομο της λέξης $\mathbf{x}$. Δηλαδή
$\mathbf{x} \cdot \mathrm{P}^{\perp} = (\sum_1^{10} x_i,\ \sum_1^{10} i\, x_i) = (\sum_1^{10} a_i + k,\ \sum_1^{10} i\, a_i + jk) =$
$= (k \mathrm{mod} 11,\ jk \mathrm{mod} 11)$. Οπότε μπορούμε όχι μόνο να διορθώσουμε το λάθος, αλλά επιπλέον να εντοπίσουμε τη θέση στην οποία υπεισήλθε το λάθος καθώς και το μέγεθος του χαρακτήρα k που προκάλεσε την αλλοίωση.

Αν κατά τη μετάδοση της λέξης επήλθε αναγραμματισμός και δύο χαρακτήρες έχουν αντιμετατεθεί στις θέσεις r και j, δηλαδή $x_r = a_j$ και $x_j = a_r$, τότε έχουμε $\mathbf{x} \cdot \mathrm{P}^{\perp} = (\sum_1^{10} a_i,\ \sum_{i=1}^{10} i \cdot a_i) + (r-j)x_j + (j-r)x_r) =$ $(0,\ (r-j)x_j + (j-r)x_r) = (0,\ (r-j)(x_j - x_r))$. Στην τελευταία ισότητα βλέπουμε ότι η πρώτη συντεταγμένη είναι ίση με 0, η δεύτερη όμως συντεταγμένη ανιχνεύει ότι επήλθε αναγραμματισμός (βλέπε παρατηρήσεις μετά το Παράδειγμα 1.3.19).

Παρατηρήσεις 2.3.18. 1. Στο τελευταίο παράδειγμα ο κώδικας $\mathcal{D}$ είναι επί του $\mathbb{Z}_{11}$. Ενδιαφέρον παρουσιάζει ο *δεκαδικός* κώδικας $\mathcal{E}$, ο οποίος προέρχεται από σμίκρυνση του κώδικα $\mathcal{D}$ αν διαγράψουμε όλες τις (κωδικο)λέξεις στις οποίες εμφανίζεται ο χαρακτήρας "10" (κάτι ανάλαγο είχαμε κάνει για τον σχηματισμό του κώδικα ISBN). Ο κώδικας $\mathcal{E}$ ως υποκώδικας του $\mathcal{D}$ έχει ελάχιστη απόσταση (τουλάχιστον) ίση με τρία και για κάθε $\mathbf{a} \in \mathcal{E}$ ικανοποιούνται οι εξισώσεις ισοτιμίας $\mathbf{a} \cdot \mathrm{P}^{\perp} = (0, 0)$, όπου φυσικά οι πράξεις εξακολουθούν να γίνονται mod11.

Ο κώδικας $\mathcal{E}$ δεν είναι γραμμικός (γιατί;), είναι όμως αρκετά μεγάλος (βλέπε άσκηση $1.5.3_4$) και είχε χρησιμοποιηθεί στο παρελθόν για την κωδικοποίηση των αριθμών τηλεφώνων. Πράγματι, υποθέτουμε ότι οι δεκαψήφιοι αριθμοί τηλεφώνου σε μια χώρα αποτελούν στοιχεία του κώδικα $\mathcal{E}$. Τότε κατά την επιλογή ενός αριθμού κλήσης, αν γίνει λάθος σε ένα μόνο ψηφίο, ο αριθμός *διορθώνεται* αυτόματα και η κλήση κατευθύνεται στον παραλή-

πτη που πράγματι ήθελε ο αποστολέας. Αν κατά την επιλογή γίνει ένας αναγραμματισμός (πράγμα σύνηθες), τότε η κλήση δεν προοθείται και ο αποστολέας ειδοποιείται (π.χ. «ο αριθμός που καλείτε δεν αντιστοιχεί σε συνδρομητή») και επαναλαμβάνει την κλήση.

2. Ας δούμε συνοπτικά τους κώδικες που αναφέρονται στα Παραδείγματα 2.2.28 και $2.3.17_2$. Όπως βλέπουμε έχουμε τον $11-$δικό κώδικα $\mathcal{C}$ με πίνακα ελέγχου ισοτιμίας τον $\mathrm{H} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \end{pmatrix}$. Επισυνάπτοντας μια γραμμή στον πίνακα H λαμβάνουμε τον πίνακα $\mathrm{P} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \end{pmatrix}$. Ο P είναι πίνακας ελέγχου ισοτιμίας του κώδικα $\mathcal{D}$, ο οποίος αποτελεί μια σμίκρυνση του κώδικα $\mathcal{C}$.

   Με την ίδια διαδικασία θα μπορούσαμε να συνεχίσουμε την σμίκρυνση επισυνάπτοντας μια επιπλέον γραμμή στον πίνακα P και να πάρουμε τον πίνακα $\mathrm{Q} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 1^2 & 2^2 & 3^2 & 4^2 & 5^2 & 6^2 & 7^2 & 8^2 & 9^2 & 10^2 \end{pmatrix}$, ο οποίος αποτελεί τον πίνακα ελέγχου ισοτιμίας ενός ακόμη *μικρότερου* κώδικα, έστω $\mathcal{F}$. Οπότε θα μπορούσαμε να συνεχίσουμε με την ίδια διαδικασία.

Οι κώδικες που αναφέρονται στην προηγούμενη παρατήρηση ανήκουν σε μια ευρεία και πολύ σημαντική οικογένεια κωδίκων, στους BSH κώδικες. Η ονομασία προέρχεται από τα αρχικά των R.C. Bose, D.K. Ray-Chaudhuri, A. Hocquenghem που τους ανακάλυψαν στα τέλη της δεκαετίας του ¨50 και στις αρχές της δεκαετίας του ¨60. Οι κώδικες αυτοί έχουν καλές ιδιότητες και παρουσιάζουν ευκολία στην αποκωδικοποίηση και διόρθωση λαθών. Το μεγάλο τους πλεονέκτημα όμως
είναι ότι μπορούν να κατασκευασθούν (υπό ορισμένες προϋποθέσεις) ώστε να έχουν μια επιθυμητή ελάχιστη απόσταση. Είναι, όπως συνηθίζεται να λέγεται κώδικες *προσχεδιασμένης* απόστασης.

Μια συστηματική μελέτη αυτών των κωδίκων είναι πέραν του σκοπού μας. Εδώ θα αρκεσθούμε στη γενίκευση των προηγούμενων παραδειγμάτων .

Έστω p ένας πρώτος αριθμός και d, n θετικοί ακέραιοι με
$3 \leq d \leq n \leq p-1$ και $a_1, a_2, \ldots, a_n$ μη μηδενικά στοιχεία του $\mathbb{Z}_p$, (άνευ βλάβης μπορούμε να υποθέσουμε ότι $a_1 = 1, a_2 = 2, \ldots, a_n = n$) σχηματίζουμε τον πίνακα $\mathrm{H} = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ a_1 & a_2 & \cdots & a_n \\ a_1^2 & a_2^2 & \cdots & a_n^2 \\ \vdots & \vdots & \cdots & \vdots \\ a_1^{d-2} & a_2^{d-2} & \cdots & a_n^{d-2} \end{pmatrix}$. Παρατηρούμε ότι κάθε $d-1$ το

πλήθος στήλες του πίνακα αυτού σχηματίζουν έναν πίνακα Vandermonde. [2] Επομένως η τάξη του πίνακα είναι ίση με $d-1$.

Έστω $\mathcal{C}$ ο κώδικας με πίνακα ελέγχου ισοτιμίας τον πίνακα H. Η ελάχιστη απόσταση του κώδικα είναι ίση με d (Πρόταση 2.2.27),δηλαδή είναι ένας $[n, n-(d-1), d]$ γραμμικός κώδικας. Το μέγεθος του κώδικα αυτού είναι ίσο με $p^{n-(d-1)}$, που ικανοποιεί το φράγμα Singleton (Θεώρημα 1.5.20). Επομένως έχουμε αποδείξει το ακολουθο θεώρημα.

Θεώρημα 2.3.19. *Έστω p πρώτος αριθμός και d, n θετικοί ακέραιοι με $3 \leq d \leq n \leq p-1$, τότε ισχύει $A_p(n, d) = p^{n-d+1}$.*

Παρατήρηση 2.3.20. Περισσότερα για γραμμικούς κώδικας που ικανοποιούν το φράγμα Singleton θα δούμε στην Παράγραφο 2.5.

2.3.5 Ασκήσεις

1. Να κατασκευάσετε μια αντιπροσωπευτική διάταξη για τον δυαδικό κώδικα με γεννήτορα πίνακα $\begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix}$. Αποκωδικοποιείστε τις λέξεις 111 και 100.

   Υπολογίστε την πιθανότητα σωστής αποκωδικοποιήσης, όταν η μετάδοση γίνεται μέσω ενός συμμετρικού δυαδικού δίαυλου επικοινωνίας με πιθανότητα (λανθαμένης) μετάδοσης ίση με p.

   Δώστε ένα παράδειγμα λέξης που περιέχει ένα λάθος και αποκωδικοποιείται λανθασμένα.

2. Να κατασκευάσετε μια αντιπροσωπευτική διάταξη για τον δυαδικό κώδικα με γεννήτορα πίνακα $\begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{pmatrix}$. Αποκωδικοποιείστε τις λέξεις 11111, 00000 και 10110.

   Υπολογίστε την πιθανότητα σωστής αποκωδικοποιήσης, όταν η μετάδοση γίνεται μέσω ενός συμμετρικού δυαδικού δίαυλου επικοινωνίας με πιθανότητα (λανθαμένης) μετάδοσης ίση με p.

   Δώστε ένα παράδειγμα λέξης που περιέχει δύο λάθη και αποκωδικοποιείται λανθασμένα και ένα παράδειγμα λέξης που περιέχει δύο λάθη, αλλά αποκωδικοποιείται σωστά.

3. Στις δύο προηγούμενες ασκήσεις, αντί να χρησιμοποιήσετε μια αντιπροσωπευτική διάταξη, να χρησιμοποιήσετε το σύνδρομο.

[2] Για τους πίνακες Vandermonde και τις ιδιότητές τους παραπέμπουμε σε όποιοδήποτε, έστω και στοιχειώδες, βιβλίο Γραμμικής Άλγεβρας.

4. Έστω ένας δυαδικός κώδικας με πίνακα ελέγχου ισοτιμίας H. Δείξτε ότι το σύνδρομο μιας λέξης που λαμβάνουμε ισούται με το άθροισμα των εκείνων των στηλών του πίνακα H που αντιστοιχούν στις θέσεις, όπου επήλθε αλλοίωση χαρακτήρων.

5. Δείξτε ότι σε έναν γραμμικό κώδικα η ακτίνα κάλυψης είναι ίση με το μέγιστο βάρος ενός αντιπροσώπου σε μια αντιπροσωπευτική διάταξη.

6. Έστω ένας τριαδικός κώδικας με γεννήτορα πίνακα $\begin{pmatrix} 1 & 1 & 1 & 0 \\ 2 & 0 & 1 & 1 \end{pmatrix}$.

   Να υπολογίσετε έναν πίνακα ελέγχου ισοτιμίας σε κανονική μορφή.

   Να αποκοδικοποιήσετε με την βοήθεια του συνδρόμου τις λέξεις

   $2121, 1201$ και 2222.

7. Έστω ο κώδικας του Παραδείγματος $2.3.17_2$. Με τη βοήθεια του συνδρόμου να αποκωδικοποιήσετε τις λέξεις 0617960587 και και 9876543210.

2.4 Διασπορά βαρών σε έναν κώδικα

Έστω $\mathcal{C}$ ένας $[n, k, d]$ γραμμικός κώδικας, με A_i θα συμβολίζουμε τον αριθμό των (κωδικο)λέξεων, οι οποίες έχουν βάρος ίσο με i. Το σύνολο $\{ A_1, A_2, \ldots, A_n \}$ ονομάζεται **διασπορά βαρών** του κώδικα $\mathcal{C}$. Το πολυώνυμο $W_{\mathcal{C}}(z) = \sum_{i=0}^{n} A_i z^i$ ονομάζεται **απαριθμητής βάρους** για τον κώδικα $\mathcal{C}$. Προφανώς ισχύει $W_{\mathcal{C}}(z) = \sum_{\mathbf{a} \in \mathcal{C}} z^{w(\mathbf{a})}$.

Στην Παράγραφο 2.3.3 είχαμε δει (Θεώρημα 2.3.13) ότι η διασπορά βαρών ενός γραμμικού κώδικα είναι σημαντική στην πιθανότητα σωστής ανίχνευσης λαθών. Η μελέτη του απαριθμητή βάρους αναδεικνύει τη δομή ενός κώδικα ως διανυσματικού χώρου και *αποκαλύπτει* μια βαθύτερη σχέση ενός γραμμικού κώδικα με τον αντίστοιχο δυϊκό κώδικα, κάτι που δεν είναι προφανές από τον ορισμό της καθετότητας και δεν μπορούμε να το συνάγουμε από τον απευθείας υπολογισμό των A_i διατρέχοντας μία προς μία τις (κωδικο)λέξεις του κώδικα.

Το κύριο αποτέλεσμα σ' αυτή την κατεύθυνση είναι το Θεώρημα του MacWilliams. Αν και η ιδέα της απόδειξης είναι σχετικά απλή, στη γενική περίπτωση παρουσιάζει δυσκολίες λόγω της πολυπλοκότητας των υπολογισμών. Εδώ θα δώσουμε μια απλή απόδειξη στην ειδική περίπτωση των δυαδικών κωδίκων. Πριν διατυπώσουμε και αποδείξουμε το αντίστοιχο Θεώρημα θα παραθέσουμε μερικά αποτελέσμα υπό μορφήν Λημμάτων, τα οποία από μόνα τους παρουσιάζουν ανεξάρτητο ενδιαφέρον.

Λήμμα 2.4.1. *Έστω $\mathcal{C}$ ένας δυαδικός $[n, k, d]$ κώδικας. Επιλέγουμε και σταθεροποιούμε ένα $\mathbf{y} \in \mathbb{Z}_2^n$ με $\mathbf{y} \notin \mathcal{C}^\perp$. Το σύνολο $A = \{\, \mathbf{x} \in \mathcal{C} \mid < \mathbf{x}, \mathbf{y} >= 0 \,\}$ είναι διανυσματικός υπόχωρος του $\mathbb{Z}_2^n$ διάστασης ίσης με $k-1$.*

Απόδειξη. Το αποτέλεσμα έπεται άμεσα από την Πρόταση 2.2.6 και το γεγονός ότι αν δύο στοιχεία $\mathbf{u}, \mathbf{v} \in \mathcal{C}$ δεν ανήκουν στο σύνολο A, τότε $\mathbf{u}-\mathbf{v} \in A$ (πάντα υπάρχει τουλάχιστον ένα στοιχείο του κώδικα που δεν ανήκει στο A, αφού το $\mathbf{y} \notin \mathcal{C}^\perp$).

□

Από το προηγούμενο λήμμα έπεται άμεσα ότι αν $\mathbf{y} \notin \mathcal{C}^\perp$, τότε ακριβώς τα μισά στοιχεία του κώδικα είναι κάθετα ως προς το $\mathbf{y}$.

Λήμμα 2.4.2. *Έστω $\mathcal{C}$ ένας δυαδικός $[n, k, d]$ κώδικας. Επιλέγουμε και σταθεροποιούμε ένα $\mathbf{y} \in \mathbb{Z}_2^n$. Τότε*

$$\sum_{\mathbf{x}\in\mathcal{C}} (-1)^{<\mathbf{x},\mathbf{y}>} = \begin{cases} 2^k & \text{αν } \mathbf{y} \in \mathcal{C}^\perp \\ 0 & \text{αν } \mathbf{y} \notin \mathcal{C}^\perp \end{cases} .$$

Απόδειξη. Αν $\mathbf{y} \in \mathcal{C}^\perp$, τότε $< \mathbf{x}, \mathbf{y} >= 0$ για κάθε $\mathbf{x} \in \mathcal{C}$, οπότε έχουμε την πρώτη περίπτωση, αφού ο κώδικας περιέχει 2^k το πλήθος στοιχεία.

Υποθέτουμε ότι $\mathbf{y} \notin \mathcal{C}^\perp$. Όπως έχουμε παρατηρήσει, για τα μισά το πλήθος στοιχεία του κώδικα ισχύει $< \mathbf{x}, \mathbf{y} >= 0$, επομένως για τα υπόλοιπα μισά θα ισχύει $< \mathbf{x}, \mathbf{y} >= 1$. Άρα έχουμε την δεύτερη περίπτωση. □

Λήμμα 2.4.3. *Επιλέγουμε και σταθεροποιούμε ένα $\mathbf{x} = x_1\, x_2 \cdots x_n \in \mathbb{Z}_2^n$. Τότε τα πολυώνυμα $\sum_{\mathbf{y}\in\mathbb{Z}_2^n} z^{w(\mathbf{y})}(-1)^{<\mathbf{x},\mathbf{y}>}$ και $(1-z)^{w(\mathbf{x})}(1+z)^{n-w(\mathbf{x})}$ είναι ίσα.*

Απόδειξη. Για το τυχαίο $\mathbf{y} = y_1\, y_2 \cdots y_n \in \mathbb{Z}_2^n$ έχουμε
$w(\mathbf{y}) = y_1 + y_2 + \cdots + y_n$ και $< \mathbf{x}, \mathbf{y} >= x_1y_1 + x_2y_2 + \cdots + x_ny_n$. Οπότε έχουμε
$\sum_{\mathbf{y}\in\mathbb{Z}_2^n} z^{w(\mathbf{y})}(-1)^{<\mathbf{x},\mathbf{y}>} = \sum_{\mathbf{y}\in\mathbb{Z}_2^n} z^{y_1+y_2+\cdots+y_n}(-1)^{x_1y_1+x_2y_2+\cdots+x_ny_n} =$
$= \sum_{\mathbf{y}\in\mathbb{Z}_2^n} (\prod_{i=1}^n z^{y_i}(-1)^{x_iy_i})$. Στο τελευταίο άθροισμα έχουμε 2^n το πλήθος προσθεταίους (τόσα είναι τα στοιχεία του $\mathbb{Z}_2^n$) και κάθε προσθεταίος είναι ένα γινόμενο με n το πλήθος όρους. Επίσης οι εκθέτες y_i λαμβάνουν τις τιμές 0 και 1. Οπότε εύκολα βλέπουμε ότι το τελευταίο άθροισμα είναι ίσο με
$\prod_{i=1}^n (\sum_{j=0}^1 z^j(-1)^{x_ij}) = \prod_{i=1}^n (1 + z(-1)^{x_i})$. Στο τελευταίο γινόμενο οι όροι $1 + z(-1)^{x_i}$ είναι της μορφής $1 + z$ αν $x_i = 0$ και της μορφής $1 - z$ αν $x_i = 1$. Το πλήθος των x_i, τα οποία ισούνται με 1 είναι όσο και το βάρος $w(\mathbf{x})$. Επομένως μπορούμε να συνεχίσουμε και το τελευταίο γινόμενο γίνεται
$\prod_{i=1}^n (1 + z(-1)^{x_i}) = (1-z)^{w(\mathbf{x})}(1+z)^{n-w(\mathbf{x})}$. Δηλαδή αποδείξαμε την αποδεικτέα σχέση $\sum_{\mathbf{y}\in\mathbb{Z}_2^n} z^{w(\mathbf{y})}(-1)^{<\mathbf{x},\mathbf{y}>} = (1-z)^{w(\mathbf{x})}(1+z)^{n-w(\mathbf{x})}$. □

Θεώρημα 2.4.4. Η ταυτότητα MacWilliams
Έστω $\mathcal{C}$ ένας δυαδικός $[n, k, d]$ κώδικας. Τότε ισχύει

$$W_{\mathcal{C}^\perp}(z) = (|\,\mathcal{C}\,|)^{-1}(1+z)^n W_{\mathcal{C}}\Big(\frac{1-z}{1+z}\Big).$$

Απόδειξη. Από το προηγούμενο λήμμα έχουμε $\sum_{\mathbf{x}\in\mathcal{C}}(\sum_{\mathbf{y}\in\mathbb{Z}_2^n} z^{w(\mathbf{y})}(-1)^{<\mathbf{x},\mathbf{y}>}) = \sum_{\mathbf{x}\in\mathcal{C}}(1-z)^{w(\mathbf{x})}(1+z)^{n-w(\mathbf{x})} = (1+z)^n \sum_{\mathbf{x}\in\mathcal{C}}(\frac{1-z}{1+z})^{w(\mathbf{x})} = (1+z)^n W_{\mathcal{C}}(\frac{1-z}{1+z})$.

Θα υπολογίσουμε το προηγούμενο (διπλό) άθροισμα αλλάζοντας τη σειρά των προσθεταίων.

$\sum_{\mathbf{x}\in\mathcal{C}}(\sum_{\mathbf{y}\in\mathbb{Z}_2^n} z^{w(\mathbf{y})}(-1)^{<\mathbf{x},\mathbf{y}>}) = \sum_{\mathbf{y}\in\mathbb{Z}_2^n} z^{w(\mathbf{y})}(\sum_{\mathbf{x}\in\mathcal{C}}(-1)^{<\mathbf{x},\mathbf{y}>})$.

Από το Λήμμα 2.4.2 έχουμε ότι το άθροισμα $\sum_{\mathbf{x}\in\mathcal{C}}(-1)^{<\mathbf{x},\mathbf{y}>} = 2^k$ μόνο για τα $\mathbf{y} \in \mathcal{C}^\perp$, οπότε συνεχίζοντας έχουμε $\sum_{\mathbf{x}\in\mathcal{C}}(\sum_{\mathbf{y}\in\mathbb{Z}_2^n} z^{w(\mathbf{y})}(-1)^{<\mathbf{x},\mathbf{y}>}) = \sum_{\mathbf{y}\in\mathcal{C}^\perp} z^{w(\mathbf{y})}2^k = 2^k W_{\mathcal{C}^\perp}(z)$.

Οπότε με απλή σύγκριση έπεται το αποτέλεσμα. □

Παρατηρήσεις 2.4.5.

1. Αλλάζοντας τον ρόλο του κώδικα $\mathcal{C}$ με τον δυϊκό του $\mathcal{C}^\perp$, για την προηγούμενη ισότητα έχουμε την εξής έκφραση

$$W_{\mathcal{C}}(z) = \frac{1}{2^{n-k}}(1+z)^n W_{\mathcal{C}^\perp}\Big(\frac{1-z}{1+z}\Big).$$

2. Η χρήση της ταυτότητας MacWilliams δεν προσφέρεται για τον άμεσο υπολογισμό του απαριθμητή βάρους ένος κώδικα. Συνήθως, όταν η διάσταση k του κώδικα είναι μικρή, μπορούμε να προχωρήσουμε στον απευθείας υπολογισμό των A_i διατρέχοντας μία προς μία τις (κωδικο)λέξεις του κώδικα. Όταν όμως η διάσταση είναι μεγάλη, η διάταση $n-k$ του δυϊκού κώδικα είναι μικρή, οπότε η χρήση της ταυτότητας MacWilliams είναι απαραίτητη και αποτελεσματική.

3. Στη γενική περίπτωση, όπου έχουμε έναν γραμμικό $[n, k, d]$ κώδικα $\mathcal{C}$ επί ενός σώματος $\mathbb{F}$ με p το πλήθος στοιχεία, τότε η ταυτότητα MacWilliams έχει τη μορφή

$$W_{\mathcal{C}^\perp}(z) = (|\,\mathcal{C}\,|)^{-1}[1+(p-1)z]^n W_{\mathcal{C}}\Big(\frac{1-z}{1+(p-1)z}\Big).$$

2.4.1 Ασκήσεις

1. Έστω $\mathcal{C}$ ένας δυαδικός γραμμικός κώδικας μήκους n. Υποθέτουμε ότι η λέξη $11\cdots1$ είναι στοιχείο του $\mathcal{C}$, δείξτε ότι $A_i = A_{n-i},\ i = 0, 1, \ldots, n$.

2. Υπολογίστε τον απαριθμητή βάρους ενός κώδικα με γενήτορα πίνακα
$\mathrm{G} = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix}$ με δύο τρόπους. Απευθείας και με τη χρήση της ταυτότητας MacWilliams.

3. Έστω $\mathcal{C}$ ένας δυαδικός γραμμικός κώδικας και $\hat{\mathcal{C}}$ ο κώδικας που προέρχεται με την επισύναψη ενός ψηφίου ελέγχου ισοτιμίας. Δείξτε ότι $W_{\hat{\mathcal{C}}}(z) = \frac{1}{2}\Big[(1+z)W_{\mathcal{C}}(z) + (1-z)W_{\mathcal{C}}(-z)\Big]$.

4. Αποδείξτε την εξής έκφραση του Θεωρήματος 2.3.13.

   Έστω $\mathcal{C}$ $[n, k, d]$ ένας δυαδικός γραμμικός κώδικας. Η πιθανότητα μη ανίχνευσης λαθών είναι ίση με
   $p(\,\mu\eta\ \alpha\nu\acute{\iota}\chi\nu\epsilon\upsilon\sigma\eta\varsigma\ \lambda\alpha\theta\acute{\omega}\nu\,) = \frac{1}{2^{n-k}} W_{\mathcal{C}^\perp}(1-2p) - (1-p)^n$.

2.5 Κώδικες με μέγιστη απόσταση (MDS Κώδικες)

Στην Παράγραφο 1.5.2 είχαμε ασχοληθεί με το δύσκολο πρόβλημα της εύρεσης του μεγέθους βέλτιστων κωδίκων. Αν έχουμε ένα αλφάβητο $\mathbb{A}$ με r το πλήθος στοιχεία και n και d φυσικούς αριθμούς, ζητούσαμε να προδιορίσουμε το μεγαλύτερο μέγεθος κώδικα που μπορεί να υπάρξει με μήκος ίσο με n και ελάχιστη απόσταση ίση με d. Δηλαδή αναζητούσαμε να προσδιορίσουμε τον αριθμό $A_r(n, d) = \max\{\, M \mid \text{υπάρχει } (n, M, d) \text{ κώδικας} \,\}$.

Ένα από τα άνω φράγματα για τον αριθμό $A_r(n, d)$ είναι το φράγμα Singleton (Θεώρημα 1.5.20), το οποίο στην περίπτωση των γραμμικών κωδίκων έχει τη μορφή. Για έναν γραμμικό $[n, k, d]$ κώδικα ισχύει $k \leq n - d + 1$ (Πρόταση 2.1.13).

Αντί να σταθεροποιήσουμε το μήκος n και την ελάχιστη απόσταση d και να αναζητήσουμε το μεγαλύτερο δυνατόν μέγεθος κώδικα που μπορεί να υπάρξει με τις παραμέτρους n και d, μπορούμε να σταθεροποιήσουμε τις παραμέτρους μήκος n και το μέγεθος M και να αναζητούμε κώδικες με τη μεγαλύτερη δυνατή ελάχιστη απόσταση και με τις παραμέτρους n και M.
Στην περίπτωση των γραμμικών κωδίκων, λόγω του ότι $d \leq n-k+1$, το τελευταίο πρόβλημα ανάγεται στην αναζήτηση κωδίκων με παραμέτρους $[n, k, n-k+1]$ (ή δυϊκά με παραμέτρους $[n, n-d+1, d]$).

Ένας γραμμικός κώδικας $\mathcal{C}$ με παραμέτρους $[n, k, n-k+1]$ θα ονομάζεται κώδικας **μέγιστης** (ελάχιστης) απόστασης (για συντομία MDS κώδικες, από το Maximum Distance Separable).

Παραδείγματα 2.5.1. 1. Προφανώς ο $p-$αδικός κώδικας $\mathcal{C} = \mathbb{F}^n$, δηλαδή όλος ο χώρος, έχει παραμέτρους $[n,\, n,\, 1]$ και είναι κώδικας μέγιστης απόστασης.

2. Ο επαναληπτικός $p-$αδικός κώδικας
$\mathcal{R}_p(n) = \{ \underbrace{00\cdots0}_{n-\text{φορές}}, \underbrace{11\cdots1}_{n-\text{φορές}}, \ldots, \underbrace{p-1\, p-1\cdots p-1}_{n-\text{φορές}} \}$ είναι ένας κώδικας μέγιστης απόστασης με παραμέτρους $[n, 1,\, n]$.

3. Έστω ένα πεπερασμένο σώμα $\mathbb{F}$ και ένας θετικός ακέραιος $n \geq 2$. Για κάθε $1 \leq i \leq n-1$ έστω η λέξη $\mathbf{e}_i$ μήκους n, η οποία έχει στις θέσεις i και $i+1$ το 1 και πάντου αλλού μηδέν. Δεν είναι δύσκολο να δούμε ότι τα $n-1$ το πλήθος $\mathbf{e}_i$ είναι γραμμικά ανεξάρτητα και επομένως ο γραμμικός κώδικας, έστω $\mathcal{C}$, που έχει αυτά ως βάση είναι ένας κώδικας με παραμέτρους $[n,\, n-1,\, 2]$, δηλαδή ένας κώδικας μέγιστης απόστασης.

   (Αν περιορισθούμε σε δυαδικούς κώδικες, τότε ο κώδικας του παραδείγματος αυτού είναι ο γνωστός κώδικας $\mathcal{A}_n$ που αποτελείται από όλες τις λέξεις αρτίου βάρους (γιατί;) (βλέπε Άσκηση $2.1.2_2$)).

4. Αν τώρα $n \geq 3$ και για κάθε $1 \leq i \leq n-2$ πάρουμε τις λέξεις $\mathbf{e}_i$ μήκους n, οι οποίες έχουν στις θέσεις i και $i+1$ και $i+2$ το 1 και πάντου αλλού μηδέν. Δεν είναι δύσκολο να δούμε ότι τα $n-2$ το πλήθος $\mathbf{e}_i$ είναι γραμμικά ανεξάρτητα και επομένως ο γραμμικός κώδικας, έστω $\mathcal{C}$, που έχει αυτά ως βάση είναι ένας κώδικας με παραμέτρους $[n,\, n-2,\, 2]$, δηλαδή δεν είναι ένας κώδικας μέγιστης απόστασης.

5. Στη σελίδα 92 είχαμε δει πως με τη βοήθεια των πινάκων Vandermonde μπορούμε να κατασκευάσουμε κώδικες μέγιστης απόστασης.

Τα τρία πρώτα παραδείγματα αποτελούν ακραίες περιπτώσεις κωδίκων μέγιστης απόστασης, κώδικες με παραμέτρους $[n,\, n,\, 1], [n, 1,\, n]$ και $[n,\, n-1,\, 2]$ θα ονομάζονται **τετριμμένοι** MDS κώδικες. Στα επόμενα θα ασχοληθούμε με κώδικες μέγιστης απόστασης και παραμέτρους $[n,\, k,\, n-k+1]$ με $2 \leq k \leq n-2$.

Από την Πρόταση 2.2.27 έχουμε έναν τρόπο υπολογισμού της ελάχιστης απόστασης ενός γραμμικού κώδικα με τη βοήθεια ενός πίνακα ελέγχου ισοτιμίας του κώδικα. Στην περίπτωση των κωδίκων μέγιστης απόστασης έχουμε τον ακόλουθο χαρακτηρισμό.

Πρόταση 2.5.2. *Έστω ένας γραμμικός $[n,\, k,\, d]$ κώδικας $\mathcal{C}$ με έναν πίνακα ελέγχου ισοτιμίας* P. *Ο κώδικας $\mathcal{C}$ είναι κώδικας μεγίστης απόστασης αν και μόνο αν οποιεσδήποτε $n-k$ το πλήθος στήλες του* P *είναι γραμμικά ανεξάρτητες.*

Απόδειξη. Η απόδειξη είναι άμεση από την Πρόταση 2.2.27.

□

Θεώρημα 2.5.3. *Ένας γραμμικός κώδικας $\mathcal{C}$ επί ενός σώματος $\mathbb{F}_p$ είναι κώδικας μέγιστης απόστασης αν και μόνο αν ο αντίστοιχος δυϊκός κώδικας $\mathcal{C}^\perp$ είναι κώδικας μέγιστης απόστασης.*

Απόδειξη. Υποθέτουμε ότι ο κώδικας $\mathcal{C}$ έχει παραμέτρους $[n, k, n-k+1]$, τότε ο δυϊκός $\mathcal{C}^\perp$ έχει παραμέτρους $[n, n-k, d]$ με $d \leq n-(n-k)+1 = k+1$. Σκοπός μας είναι να αποδείξουμε ότι $d = k+1$.

Υποθέτουμε ότι $d \leq k$, τότε υπάρχει μια (κωδικο)λέξη $\mathbf{c}$ στον κώδικα με βάρος ίσο με d, δηλαδή η $\mathbf{c}$ σε d το πλήθος θέσεις έχει μη μηδενικούς χαρακτήρες.

Έστω P ένας πίνακας ελέγχου ισοτιμίας του κώδικα $\mathcal{C}$, τότε αυτός είναι γεννήτορας πίνακας για τον δυϊκό κώδικα $\mathcal{C}^\perp$, επομένως υπάρχει $\mathbf{a} \in \mathbb{F}_p^{n-k}$ έτσι ώστε $\mathbf{c} = \mathbf{a}\mathrm{P}$. Από τον πίνακα P διαγράφουμε k το πλήθος στήλες ως εξής, διαγράφουμε d το πλήθος στήλες στις αντίστοιχες θέσεις που στην (κωδικο)λέξη $\mathbf{c}$ εμφανίζονται μη μηδενικοί χαρακτήρες και τις υπόλοιπες $k-d$ τυχαία (έχουμε υποθέσει ότι $d \leq k$). Ο υποπίνακας $\bar{\mathrm{P}}$ που προκύπτει είναι τετραγωνικός $(n-k)\times(n-k)$ πίνακας και από την προηγούμενη πρόταση έχουμε ότι είναι αντιστρέψιμος. Από τον τρόπο διαγραφής των k στηλών του πίνακα για τη δημιουργία του $\bar{\mathrm{P}}$ και το γεγονός ότι $\mathbf{c} = \mathbf{a}\mathrm{P}$ έπεται ότι $\mathbf{a}\bar{\mathrm{P}} = \mathbf{0}$. Ο πίνακας $\bar{\mathrm{P}}$ είναι αντιστρέψιμος, άρα $\mathbf{a} = \mathbf{0}$, δηλαδή $\mathbf{c} = \mathbf{a}\mathrm{P} = \mathbf{0}$, άτοπο. Επομένως δεν ισχύει η υπόθεση $d \leq k$. Άρα $d = k+1$.

□

Από τα προηγούμενα, επειδή κάθε γεννήτορας πίνακας ενός κώδικα είναι πίνακας ελέγχου ισοτιμίας του αντίστοιχου δυϊκού και αντίστροφα, έχουμε το ακόλουθο πόρισμα.

Πόρισμα 2.5.4. *Ένας γραμμικός $[n, k, d]$ κώδικας είναι κώδικας μέγιστης απόστασης αν και μόνο αν σε έναν γεννήτορα πίνακα κάθε k το πλήθος στήλες είναι γραμμικά ανεξάρτητες.*

Θεώρημα 2.5.5. *Ένας γραμμικός $[n, k, d]$ κώδικας $\mathcal{C}$ με γεννήτορα πίνακα $\mathrm{G} = [\mathrm{I}_k \quad \mathrm{A}]$ είναι κώδικας μέγιστης απόστασης αν και μόνο αν κάθε τετραγωνικός υποπίνακας του A είναι αντιστρέψιμος.*

Απόδειξη. Υποθέτουμε ότι κάθε τετραγωνικός υποπίνακας του πίνακα A είναι αντιστρέψιμος. Ο πίνακας A είναι ένας $k \times (n-k)$ πίνακας. Αν $k \leq n-k$, τότε κάθε k το πλήθος από τις στήλες του A είναι γραμμικά ανεξάρτητες. Αν $n-k \leq k$, τότε όλες οι στήλες του A είναι γραμμικά ανεξάρτητες. Έστω k το πλήθος στήλες του γεννήτορα πίνακα G. Αν αυτές είναι οι πρώτες στήλες,

προφανώς είναι γραμμικά ανεξάρτητες. Αν όλες είναι στήλες του πίνακα A, τότε από τα προηγούμενα είναι γραμμικά ανεξάρτητες. Υποθέτουμε ότι έχουμε k το πλήθος στήλες από τον πίνακα G, οι οποίες δεν είναι γραμμικά ανεξάρτητες, τότε μερικές από αυτές θα είναι στήλες του πίνακα I_k και μερικές θα είναι στήλες του A. Άρα μια από τις στήλες του I_k θα είναι γραμμικός συνδυασμός κάποιων στηλών του πίνακα I_k και κάποιων στηλών του πίνακα A με τουλάχιστον μια από τις στήλες του πίνακα A να έχει μη μηδενικό συντελεστή (γιατί;). Από τις στήλες αυτές διαγράφουμε τις θέσεις στις οποίες εμφανίζεται το 1. Τότε προκύπτει ένας γραμμικός συνδυασμός της μηδενικής στήλης με τμήματα στηλών του πίνακα A δηλαδή υπάρχει τετραγωνικός υποπίνακας του A που δεν είναι αντιστρέψιμος, άτοπο. Άρα κάθε k το πλήθος στήλες του πίνακα G είναι γραμμικά ανεξάρτητες και ο κώδικας είναι κώδικας μέγιστης απόστασης από το προηγούμενο πόρισμα.

Αντίστροφα, υποθέτουμε ότι ο κώδικας είναι κώδικας μέγιστης απόστασης. Έστω ένας B $\nu \times \nu$ υποπίνακας του πίνακα A. Μεταθέτοντας τις γραμμές και στήλες του πίνακα G μπορούμε να πάρουμε έναν $k \times n$ πίνακα της μορφής $\hat{\mathrm{G}} = \begin{bmatrix} \mathbf{0} & \mathrm{B} & * \\ \mathrm{I}_{k-\nu} & * & * \end{bmatrix}$, όπου τα $*$ παριστούν πίνακες καταλλήλων διαστάσεων. Ο πίνακας $\hat{\mathrm{G}}$ είναι γεννήτορας πίνακας ενός κώδικα ισοδυνάμου με τον κώδικα $\mathcal{C}$, επομένως και ο νέος κώδικας είναι κώδικας μέγιστης απόστασης (ισοδύναμοι κώδικες έχουν την ίδια ελάχιστη απόσταση). Από το προηγούμενο πόρισμα έχουμε ότι οι πρώτες k το πλήθος στήλες του πίνακα $\hat{\mathrm{G}}$ είναι γραμμικά ανεξάρτητες επομένως οι στήλες του πίνακα B είναι γραμμικά ανεξάρτητες (γιατί;), άρα ο πίνακας B είναι αντιστρέψιμος.

□

Μια άμεση παρατήρηση είναι ότι σε έναν κώδικα μέγιστης απόστασης με γεννήτορα πίνακα $\mathrm{G} = [\mathrm{I}_k \quad \mathrm{A}]$ κανένα στοιχείο του πίνακα A δεν είναι μηδενικό.

Συνοψίζοντας όλα τα προηγούμενα μπορούμε να δώσουμε τους εξής ισοδύναμους χαρακτηρισμούς ενός κώδικα μέγιστης απόστασης.

Θεώρημα 2.5.6. *Έστω ένας $[n, k, d]$ κώδικας $\mathcal{C}$. Τα ακόλουθα είναι ισοδύναμα.*

1. *Ο κώδικας $\mathcal{C}$ είναι μέγιστης απόστασης.*
2. *Οποιεσδήποτε k το πλήθος γραμμές ενός γεννήτορα πίνακα του $\mathcal{C}$ είναι γραμμικά ανεξάρτητες.*
3. *Οποιεσδήποτε $n-k$ το πλήθος γραμμές ενός πίνακα ελέγχου ισοτιμίας του $\mathcal{C}$ είναι γραμμικά ανεξάρτητες.*
4. *Ο δυϊκός κώδικας $\mathcal{C}^{\perp}$ είναι κώδικας μέγιστης απόστασης.*

5. *Αν* $\mathrm{G} = [\mathrm{I}_k \quad \mathrm{A}]$ *είναι ένας γεννήτορας πίνακας του* $\mathcal{C}$ *σε κανονική μορφή, τότε κάθε τετραγωνικός υποπίνακας του* A *είναι αντιστρέψιμος.*

Παράδειγμα 2.5.7. Έστω ο πίνακας $\mathrm{A} = \begin{pmatrix} 1 & 6 & 2 & 5 & 1 \\ 1 & 4 & 3 & 3 & 6 \\ 1 & 5 & 5 & 1 & 5 \end{pmatrix}$ επί του σώματος $\mathbb{Z}_7$. Μπορούμε να ελέγξουμε ότι κάθε τετραγωνικός υποπίνακας του A είναι αντιστρέψιμος (κάντε το!), άρα μπορούμε να κατασκευάσουμε δύο κώδικες μέγιστης απόστασης επί του $\mathbb{Z}_7$, έναν $[8, 3, 6]$ κώδικα με γεννήτορα πίνακα $[\mathrm{I}_3 \quad \mathrm{A}]$ και έναν $[8, 5, 4]$ κώδικα με πίνακα ελέγχου ισοτιμίας τον πίνακα $[\mathrm{A} \quad \mathrm{I}_3]$.

Στο τελευταίο θεώρημα έχουμε ισοδύναμους χαρακτηρισμούς για έναν κώδικα μέγιστης απόστασης, αλλά δεν έχουμε συνθήκες για το αν υπάρχουν μη τετριμμένοι κώδικες μέγιστης απόστασης με δεδομένο μήκος n και δεδομένη διάσταση k. Η μόνη συνθήκη που έχουμε είναι ότι για μη τετριμμένους κώδικες μέγιστης απόστασης πρέπει να ισχύει $2 \leq k \leq n-2$. Θα δούμε ότι η απαίτηση η ελάχιστη απόσταση του κώδικα πρέπει να είναι ίση με $d = n - k + 1$ περιορίζει κατά πολύ τη δυνατότητα υπάρξης κωδίκων μέγιστης απόστασης και έχει σχέση με το μέγεθος του πεπερασμένου σώματος $\mathbb{F}_p$ επί του οποίου ορίζεται ο κώδικας.

Θεώρημα 2.5.8. *Έστω ένα πεπερασμένο σώμα* $\mathbb{F}_p$ *με* $|\,\mathbb{F}_p\,| = q$. *Δεν υπάρχει μη τετριμμένος* $[n, k, d]$ *κώδικας μέγιστης απόστασης με* $2 \leq k \leq n - q$.

Απόδειξη. Υποθέτουμε ότι επί του σώματος $\mathbb{F}_p$ υπάρχει ο κώδικας $\mathcal{C}$ ελάχιστης απόστασης με παραμέτρους $[n, k, n-k+1]$ και ότι $2 \leq k \leq n - q$. Έστω $\mathrm{G} = [\mathrm{I}_k \; \mathrm{A}]$ ένας γεννήτορας πίνακας σε κανονική μορφή. Ο πίνακας A έχει $n - k \geq q$ το πλήθος στήλες. Όπως έχουμε παρατηρήσει, κανένα στοιχείο του A δεν είναι 0. Οπότε πολλαπλασιάζοντας κάθε στήλη του A με το αντίστροφο του πρώτου στοιχείου της λαμβάνουμε έναν πίνακα $\hat{\mathrm{A}}$, του οποίου τα στοιχεία της πρώτης γραμμής είναι όλα 1. Ο κώδικας με γεννήτορα πίνακα $\hat{\mathrm{G}} = [\mathrm{I}_k \; \hat{\mathrm{A}}]$ είναι ισοδύναμος με τον αρχικό κώδικα, άρα είναι κώδικας μέγιστης απόστασης. Επειδή υποθέσαμε ότι $n - k \geq q$, δηλαδή το πλήθος των στηλών είναι μεγαλύτερο από το πλήθος των στοιχείων του αλφαβήτου, προφανώς στη δεύτερη γραμμή (και σε κάθε γραμμή) του πίνακα $\hat{\mathrm{A}}$ δύο τουλάχιστον στοιχεία θα είναι ίσα. Πολλαπλασιάζουμε την πρώτη γραμμή του πίνακα $\hat{\mathrm{G}}$ με το στοιχείο, το οποίο εμφανίζεται στη δεύτερη γραμμή (τουλάχιστον) δύο φορές και την αφαιρούμε από την δεύτερη γραμμή. Τότε προκύπτει μία (κωδικο)λέξη η οποία στις k πρώτες θέσεις έχει $k-2$ το πλήθος μηδενικά και στις υπόλοιπες $n-k$ θέσεις τουλάχιστον δύο μηδενικά, άρα συνολικά έχει τουλάχιστον k το πλήθος μηδενικά, δηλαδή η απόστασή της από την μηδενική (κωδικο)λέξη είναι το πολύ ίση με $n-k$. Αυτό είναι άτοπο, διότι υποθέσαμε ότι ο κώδικας είναι μέγιστης απόστασης ($d = n - k + 1$). Άρα δεν υπάρχει κώδικας μέγιστης απόστασης με $2 \leq k \leq n - q$.

□

Αν στο προηγούμενο θεώρημα αντί κου κώδικα $\mathcal{C}$ πάρουμε τον δυϊκό του, τότε έχουμε.

Πόρισμα 2.5.9. *Έστω ένα πεπερασμένο σώμα $\mathbb{F}_p$ με $\mid \mathbb{F}_p \mid = q$. Δεν υπάρχει μη τετριμμένος $[n, k, d]$ κώδικας μέγιστης απόστασης με $q \leq k \leq n$.*

Οπότε, αν υπάρχει ένας μη τετριμμένος $[n, k, d]$ κώδικας μέγιστης απόστασης, τότε αναγκαστικά $n - q + 1 \leq k \leq q - 1$.

Την τελευταία σχέση θα μπορούσαμε να την εκφράσουμε διαφορετικά ως εξής: Αν υπάρχει ένας μη τετριμμένος $[n, k, d]$ κώδικας μέγιστης απόστασης, τότε αναγκαστικά $2 \leq k \leq q - 1$ και $2 \leq n - k \leq q - 1$.

Από τα προηφούμενα έπεται το πόρισμα.

Πόρισμα 2.5.10. *Οι μόνοι δυαδικοί κώδικες μέγιστης απόστασης είναι οι τετριμμένοι.*

Έχοντας υπ' όψη τη σχέση $n - q + 1 \leq k \leq q - 1$, δηλαδή $n \leq k + q - 1$, γεννάται το ερώτημα: Δοθέντων των k και q να βρεθεί η μεγαλύτερη δυνατή τιμή του n έτσι ώστε να υπάρχει ένας κώδικας μέγιστης απόστασης με μήκος n.

Ας συμβολίσουμε με $m(k, q)$ τη μεγαλύτερη δυνατή τιμή του n. Υπάρχει η εικασία ότι $m(k, q) = q + 1$, εκτός από την περίπτωση $k = 3$, όπου έχει αποδειχθεί ότι $m(3, q) = q + 1$ αν το q είναι περιττός και $m(3, q) = q + 2$ αν το q είναι άρτιος.

Η εικασία αυτή έχει αποδειχθεί για $k \leq 5$ και όλα τα q. Για όλα τα k με $q \leq 11$ και για όλα τα περιττά $q > (4k - 9)^2$. Χρησιμοποιώντας το γεγονός ότι ένας κώδικας είναι κώδικας μέγιστης απόστασης αν και μόνο αν ο αντίστοιχος δυϊκός κώδικας είναι κώδικας μέγιστης απόστασης η εικασία έχει αποδειχθεί και σε άλλες περιπτώσεις.

Εδώ δεν θα σχοληθούμε με την απόδειξη των περιπτώσεων, όπου η εικασία ισχύει (ούτε και στις περιπτώσεις, όπου η απόδειξη είναι απλή). Θα αναδιατυπώσουμε όμως το πρόβλημα της εύρεσης της μέγιστης τιμής $m(k, q)$ του μήκους για κώδικες μέγιστης απόστασης σε ισοδύναμα προβλήματα της Γραμμικής Άλγεβρας.

Έστω ένα πεπερασμένο σώμα $\mathbb{F}_p$ με $\mid \mathbb{F}_p \mid = q$ και k ένας θετικός ακέραιος.

Τα επόμενα προβλήματα είναι ισοδύναμα με την εύρεση της μεγαλύτερης δυνατής τιμής του n, ώστε να υπάρχει κώδικας επί του $\mathbb{F}_p$ με παραμέτρους $[n, k, n - k + 1]$.

1 Να βρεθεί η μεγαλύτερη τιμή του n ώστε να υπάρχει ένας $k \times n$ πίνακας με στοιχεία από το σώμα $\mathbb{F}_p$ με την ιδιότητα κάθε υποσύνολο με k το πλήθος στήλες να είναι γραμμικά ανεξάρτητο.

2 Έστω ένας διανυσματικός χώρος V επί του σώματος $\mathbb{F}_p$ με διάσταση ίση με k να βρεθεί η μεγαλύτερη τιμή n ώστε να υπάρχει υποσύνολο του V με n το πλήθος στοιχεία και κάθε υποσύνολό του με k το πλήθος στοιχεία να αποτελεί βάση του V.

3 Να βρεθεί η μεγαλύτερη τιμή του n ώστε να υπάρχει ένας $k \times (n-k)$ πίνακας A με στοιχεία από το σώμα $\mathbb{F}_p$ με την ιδιότητα κάθε τετραγωνικός υποπίνακας του A να είναι αντιστρέψιμος.

2.5.1 Ασκήσεις

1. Έστω $\mathcal{C}$ ο κώδικας επί του $\mathbb{Z}_3$ με γεννήτορα πίνακα $\mathrm{G} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 2 \end{pmatrix}$. Δείξτε ότι $\mathcal{C}$ είναι κώδικας μέγιστης απόστασης.

2. Εξετάστε αν ο τριαδικός κώδικας $\mathcal{C}$ με γεννήτορα πίνακα $\mathrm{G} = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 2 & 1 \end{pmatrix}$ είναι κώδικας μέγιστης απόστασης.

3. Έστω α μια πρωταρχική κυβική ρίζα της μονάδας, ως γνωστόν το σύνολο $\mathbb{F} = \{\, 0,\, 1,\, \alpha,\, \alpha^2 \,\}$ είναι σώμα. Δείξτε ότι ο κώδικας $\mathcal{C}$ επί του $\mathbb{F}$ με γεννήτορα πίνακα $\mathrm{G} = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & \alpha & \alpha^2 \end{pmatrix}$ είναι κώδικας μέγιστης απόστασης.

4. Να κατασκευάσετε έναν τριαδικό κώδικα μέγιστης απόστασης με μήκος 4 και διάσταση 2.

5. Εξετάστε αν υπάρχουν τριαδικοί κώδικες μέγιστης απόστασης με παραμέτρους $[5,\, 3,\, d]$, $[6,\, 3,\, d]$ και $[n,\, 2,\, d]$ για $n \geq 5$.

6. Να κατασκευάσετε όλους τους κώδικες μέγιστης απόστασης επί του $\mathbb{Z}_5$ με διάσταση 2 και μήκη 4, 5, 6.
   Υπάρχει πενταδικός κώδικας μέγιστης απόστασης με διάσταση 2 και μήκος $n \geq 7$;

7. Για $k \geq 2$ να κατασκευάσετε κώδικες μέγιστης απόστασης επί του $\mathbb{Z}_{11}$ με μήκος n όσο το δυνατόν μεγαλύτερο.

2.6 Μερικές κατηγορίες γραμμικών κωδίκων

Στα προηγούμενα ασχοληθήκαμε με τους γραμμικούς κώδικες και είδαμε πώς η δομή ενός γραμμικού κώδικα ως διανυσματικού χώρου καθιστά τις διαδικασίες κωδικοποίησης και αποκωδικοποίησης περισσότερο αποτελεσματικές. Εδώ θα

ασχοληθούμε με ειδικές κατηγορίες γραμμικών κωδίκων. Ο τρόπος, με τον οποίο ορίζονται, τους καθιστά εύχρηστους ως προς τον χειρισμό τους. Για το λόγο αυτό παρουσιάζουν τόσο θεωρητικό, όσο και πρακτικό ενδιαφέρον.

2.6.1 Πολυωνυμικοί κώδικες

Έστω $\mathbb{F}_{k-1}[x]$ το σύνολο όλων των πολυωνύμων με βαθμό μικρότερο ή ίσον του $k-1$ και συντελεστές από το (όχι κατ' ανάγκη πεπερασμένο) σώμα $\mathbb{F}$. [3]

Πρόταση 2.6.1. *Έστω* $\alpha(x) = a_0 + a_1x + \cdots + a_{m-1}x^{m-1} \in \mathbb{F}_{m-1}[x]$, *η απεικόνιση* $\psi : \mathbb{F}_{m-1}[x] \longrightarrow \mathbb{F}^m$ *με* $\psi(\alpha(x)) = (a_0, a_1, \ldots, a_{m-1})$ *είναι ένας ισομορφισμός διανυσματικών χώρων.*

Απόδειξη. Η απόδειξη είναι απλή και αφίνεται ως άσκηση. □

Από την προηγούμενη πρόταση βλέπουμε ότι μπορούμε να ταυτίσουμε πολυώνυμα με διατεταγμένες $m-$άδες και αντίστροφα διατεταγμένες $m-$άδες με πολυώνυμα. Κατά συνέπεια, όπως θα δούμε, κώδικες με σύνολα πολυωνύμων.

Έστω p ένας πρώτος αριθμός, στα επόμενα, για ευκολία στο συμβολισμό, με $\mathbb{F}$ θα συμβολίζουμε το πεπερασμένο σώμα $\mathbb{F}_p$ και κάθε κώδικας θα θεωρείται επί του αλφαβήτου $\mathbb{F}$

Επιλέγουμε και σταθεροποιούμε ενα μη μηδενικό πολυώνυμο
$\gamma(x) = c_0 + c_1x + \cdots + c_kx^k \in \mathbb{F}_k[x]$. Για κάθε
$\alpha(x) = a_0 + a_1x + \cdots + a_{m-1}x^{m-1} \in \mathbb{F}_{m-1}[x]$ το πολυώνυμο $\alpha(x) \cdot \gamma(x)$ είναι ένα πολυώνυμο βαθμού το πολύ $m + k - 1$.

Πρόταση 2.6.2. *Η απεικόνιση* $\vartheta : \mathbb{F}_{m-1}[x] \longrightarrow \mathbb{F}_{m+k-1}[x]$ *με* $\vartheta(\alpha(x)) = \alpha(x) \cdot \gamma(x)$ *είναι μια 1 - 1 γραμμική απεικόνιση. Επομένως η εικόνα* $\vartheta(\mathbb{F}_{m-1}[x])$ *είναι ένας διανυσματικός υπόχωρος του* $\mathbb{F}_{m+k-1}[x]$ *διάστασης* m.

Απόδειξη. Για $\alpha(x), \beta(x) \in \mathbb{F}_{m-1}[x]$ και $\lambda, \mu \in \mathbb{F}$ ως γνωστόν ισχύει
$(\lambda\alpha(x) + \mu\beta(x)) \cdot \gamma(x) = \lambda(\alpha(x) \cdot \gamma(x)) + \mu(\beta(x)) \cdot \gamma(x))$. Οπότε έπεται το αποτέλεσμα.

□

Έστω $\alpha(x) \cdot \gamma(x) = r_0 + r_1x + \cdots r_{m+k-1}x^{m+k-1}$. Σύμφωνα με την Πρόταση 2.6.1 μπορούμε να ταυτίσουμε το στοιχείο $\alpha(x) \cdot \gamma(x)$ του διανυσματικού χώρου $\vartheta(\mathbb{F}_{m-1}[x])$ με το στοιχείο $(r_0, r_1, \ldots, r_{m+k-1})$ του $\mathbb{F}^{m+k}$.

Τα προηγούμενα θα μπορούσαν να εκφρασθούν ως εξής

[3] Εδώ θεωρούμε γνωστές τις έννοιες, όπως βαθμός πολυωνύμου, πρόσθεση και πολλαπλασιασμός πολυωνύμων καθώς και διαίρεση πολυωνύμων.

$$\mathbb{F}^m \xrightarrow{\psi^{-1}} \mathbb{F}_{m-1}[x] \xrightarrow{\vartheta} \mathbb{F}_{m+k-1}[x] \xrightarrow{\psi} \mathbb{F}^{m+k} .$$

Προσοχή! Στην προηγούμενη σχέση η συνάρτηση ψ^{-1} εφαρμόζεται από το $\mathbb{F}^m$ στο $\mathbb{F}_{m-1}[x]$, ενώ η συνάρτηση ψ από το $\mathbb{F}_{m+k-1}[x]$ στο $\mathbb{F}^{m+k}$. Αυτό **δεν** πρέπει να προκαλεί σύγχυση καθότι, γενικά, με ψ θα συμβολίζουμε την απεικόνιση που απεικονίζει ένα (οποιοδήποτε) πολυώνυμο στο αντίστοιχο "διάνυσμα" των συντελεστών του.

Ορισμός 2.6.3. *Το σύνολο* $\mathcal{C} = \{\, \psi(\vartheta(\alpha(x))) = \psi(\alpha(x)\cdot\gamma(x)) = \\ = (r_0, r_1, \ldots, r_{m+k-1}) \mid \alpha(x) \in \mathbb{F}_m[x] \,\}$ *θα λέγεται ένας* **πολυωνυμικός κώδικας** *με γεννήτορα πολυώνυμο (ή πολυώνυμο κωδικοποίησης) το πολυώνυμο* $\gamma(x)$.

Από τα προηγούμενα έπεται η εξής πρόταση.

Πρόταση 2.6.4. *Ένας πολυωνυμικός κώδικας είναι ένας γραμμικός κώδικας.*

Παρατηρήσεις 2.6.5.

1. Οι παράμετροι ενός πολυωνυμικού κώδικα εξαρτώνται τόσο από το γεννήτορα πολυώνυμο, όσο και από το φυσικό αριθμό m που χαρακτηρίζει το χώρο $\mathbb{F}_{m-1}[x]$, ο οποίος είναι το πεδίο ορισμού της συνάρτησης ϑ. Συγκεκριμένα το μήκος του είναι ίσο με $n = m + k$ και η διάστασή του ίση με m.

2. Αν ως πηγή (βλέπε σελίδα 8) πάρουμε το σύνολο $\mathbb{F}^m$, τότε η συνάρτηση κωδικοποίησης είναι η σύνθεση των απεικονίσεων ψ^{-1}, ϑ και ψ, δηλαδή $f = \psi \circ \vartheta \circ \psi^{-1}$

3. Πολλές φορές στα επόμενα θα *ταυτίζουμε*, όπως προείπαμε, χωρίς ιδιαίτερη μνεία, τις (κωδικο)λέξεις με πολυώνυμα, όπως και τα στοιχεία της πηγής με πολυώνυμα. (Για το λόγο αυτό οι δείκτες στην αρίθμηση των χαρακτήρων σε μια (κωδικο)λέξη θα αρχίζουν από το 0).

4. Η ελάχιστη απόσταση ενός πολυωνυμικού κώδικα είναι ίση με το μικρότερο πλήθος των μη μηδενικών συντελεστών των πολυωνύμων $\alpha(x)\cdot\gamma(x)$, όπου $\alpha(x) \in \mathbb{F}_{m-1}[x]$. Η απόδειξη δεν είναι δύσκολη, αρκεί να θυμηθούμε το Θεώρημα 2.1.3.

5. Έστω $\gamma(x) = c_0 + c_1x + \cdots + c_kx^k$ το πολυώνυμο γεννήτορας ενός πολυωνυμικού κώδικα, αν ο σταθερός όρος c_0 είναι μηδέν, τότε σε όλες τις (κωδικο)λέξεις ο πρώτος χαρακτήρας είναι μηδέν, όμοια, αν ο συντελεστής c_k είναι μηδέν, τότε ο τελευταίος χαρακτήρας σε όλες τις (κωδικο)λέξεις είναι μηδέν. Αλλά τότε οι χαρακτήρες αυτοί δεν προσφέρουν τίποτε στην

κωδικοποίηση, οπότε ο κώδικας μπορεί να συμπτυχθεί ως προς αυτές τις συντεταγμένες (βλέπε σελίδα 37). Επομένως στα επόμενα θα υποτίθεται ότι ο σταθερός όρος και ο μεγιστοβάθμιος συντελεστής στο γεννήτορα πολυώνυμο είναι μη μηδενικοί.

Παράδειγμα 2.6.6. Έστω το πολυώνυμο $\gamma(x) = 1 + x + x^3 \in \mathbb{Z}_2[x]$ και $\mathcal{C}$ ο αντίστοιχος πολυωνυμικός κώδικας μήκους 6. Ας υπολογίσουμε τα στοιχεία του και ταυτόχρονα τη συνάρτηση κωδικοποίησης f από την πηγή $\mathbb{Z}_2^3$ στον κώδικα $\mathcal{C}$.

Έστω $(a_0, a_1, a_2) \in \mathbb{Z}_2^3$, σχηματίζουμε το πολυώνυμο $\alpha(x) = a_0 + a_1x + a_2x^2$ και κάνουμε τον πολλαπλασιασμό $\alpha(x) \cdot \gamma(x) = a_0 + (a_0 + a_1)x + (a_1 + a_2)x^2 + (a_0 + a_2)x^3 + a_1x^4 + a_2x^5$. Επομένως η συνάρτηση κωδικοποίησης είναι η $f(a_0, a_1, a_2) = (a_0, a_0 + a_1, a_1 + a_2, a_0 + a_2, a_1, a_2)$ και ο κώδικας $\mathcal{C} = \{ (a_0, a_0 + a_1, a_1 + a_2, a_0 + a_2, a_1, a_2) \mid (a_0, a_1, a_2) \in \mathbb{Z}_2^3 \}$.

Ας υπολογίσουμε έναν γεννήτορα πίνακα του κώδικα $\mathcal{C}$. Τα στοιχεία $(1, 0, 0)$, $(0, 1, 0)$, $(0, 0, 1)$ αποτελούν μια βάση του $\mathbb{Z}_2^3$ και η απεικόνιση f είναι 1 - 1, επομένως οι εικόνες των στοιχείων της βάσης μέσω της f αποτελούν μια βάση του κώδικα. Έχουμε ότι $f(1, 0, 0) = (1, 1, 0, 1, 0, 0)$, $f(0, 1, 0) = (0, 1, 1, 0, 1, 0)$, $f(0, 0, 1) = (0, 0, 1, 1, 0, 1)$. Άρα ένας γεννήτορας πίνακας του $\mathcal{C}$ είναι ο $\mathrm{G} = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}$.

Ένας πίνακας ελέγχου ισοτιμίας για τον κώδικα $\mathcal{C}$ είναι ο πίνακας $\mathrm{P} = \begin{pmatrix} 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$ καθότι ισχύει $\mathrm{GP}^t = \mathbf{0}$ (Πρόταση 2.2.12).

Η ελάχιστη απόσταση του κώδικα είναι ίση με 3, σύμφωνα με την Πρόταση 2.2.27, (η πρώτη, δεύτερη και τέταρτη στήλη είναι γραμμικά εξαρτημένες, ενώ ανά δύο όλες οι στήλες είναι γραμμικά ανεξάρτητες).

Πρόταση 2.6.7. *Έστω $\mathcal{C}$ ένας πολυωνυμικός κώδικας μήκους n με γεννήτορα πολυώνυμο το $\gamma(x) = c_0 + c_1x + \cdots + c_kx^k$, ένας γεννήτορας πίνακας του $\mathcal{C}$ είναι ο $(n-k) \times n$ πίνακας* $\mathrm{G} = \begin{pmatrix} c_0 & c_1 & \cdots & c_k & 0 & 0 & \cdots & 0 \\ 0 & c_0 & \cdots & c_{k-1} & c_k & 0 & \cdots & 0 \\ \vdots & \vdots & \cdots & \vdots & \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & 0 & c_0 & c_1 & \cdots & c_k \end{pmatrix}$

Απόδειξη. Η διάσταση του κώδικα $\mathcal{C}$ είναι ίση με $m = n - k$.
Στην πρώτη γραμμή του πίνακα G τις $k+1$ πρώτες θέσεις καταλαμβάνουν οι συντελεστές του $c_0, c_1, \ldots, c_k$ του γεννήτορα πολυωνύμου και οι υπόλοιπες θέσεις είναι μηδενικά. Κάθε επόμενη γραμμή σχηματίζεται με μια κυκλική μετάθεση των

στοιχείων της αμέσως προηγούμενης γραμμής έως ότου φθάσουμε στην τελευταία γραμμή, όπου οι τελευταίες $k+1$ θέσεις είναι $c_0, c_1, \ldots, c_k$. Επομένως η τάξη του πίνακα είναι ίση με m.

Ο πολλαπλασιασμός ενός στοιχείου $(a_0, a_1, \ldots, a_{m-1}) \in \mathbb{F}^m$ (από αριστερά) με τον πίνακα G δίνει τους συντελεστές του γινομένου $\alpha(x)\cdot\gamma(x)$, όπου $\alpha(x) = a_0 + a_1x + \cdots + a_{m-1}x^{m-1} \in \mathbb{F}_{m-1}[x]$ και $\gamma(x) = c_0 + c_1x + \cdots + c_kx^k$ το πολυώνυμο γεννήτορας. Άρα ο κώδικας $\mathcal{C}$ συμπίπτει με τον κώδικα που έχει τον πίνακα G ως γεννήτορα πίνακα.

□

Έχουμε δεί στην παράγραφο 2.3.3 ότι σε ένα γραμμικό κώδικα μήκους n ένα διάνυσμα λάθους $\mathbf{e} = e_0\,e_1\cdots e_{n-1}$ δεν ανιχνεύεται αν και μόνο αν και αυτό είναι μια (κωδικο)λέξη. Για τους πολυωνυμικούς κώδικες έχουμε.

Πρόταση 2.6.8. *Σε έναν πολυωνυμικό κώδικα $\mathcal{C}$ ένα διάνυσμα λάθους $\mathbf{e} = e_0\,e_1\cdots e_{n-1}$ δεν ανιχνεύεται αν και μόνο αν το αντίστοιχο πολυώνυμο $e(x) = e_0 + e_1x + \cdots + e_{n-1}x^{n-1}$ είναι πολλαπλάσιο του γεννήτορα πολυωνύμου του κώδικα.*

Απόδειξη. Η απόδειξη είναι άμεση συνέπεια των προηγουμένων και αφίνεται ως άσκηση. □

Πρόταση 2.6.9. *Έστω ένας πολυωνυμικός κώδικας $\mathcal{C}$ μήκους n με γεννήτορα πολυώνυμο $\gamma(x)$. Υποθέτουμε ότι το $\gamma(x)$ δεν διαιρεί κανένα πολυώνυμο της μορφής $x^r + c \in \mathbb{F}_{n-1}[x]$. Τότε η ελάχιστη απόσταση του $\mathcal{C}$ είναι τουλάχιστον τρία.*

Απόδειξη. Έστω $\gamma(x) = c_0 + c_1x + \cdots + c_kx^k$, κάθε στοιχείο του κώδικα διαιρείται από το $\gamma(x)$. Πρέπει να αποδείξουμε ότι δεν υπάρχει (κωδικο)λέξη με βάρος το πολύ 2. Από την Παρατήρηση $2.6.5_4$ έπεται ότι αρκεί να αποδείξουμε ότι δεν υπάρχουν πολυώνυμα της μορφής $x^i + cx^j \in \mathbb{F}_{n-1}[x]$ με $i > j$ τα οποία να διαιρούνται από το $\gamma(x)$. Επειδή $c_0 \neq 0$ (βλέπε Παρατήρηση $2.6.5_5$), έχουμε ότι τα πολυώνυμα $\gamma(x)$ και x^ℓ είναι σχετικά πρώτα για κάθε ℓ. Επομένως αν υποθέσουμε ότι ένα πολυώνυμο της μορφής $x^i + cx^j = x^j(x^{i-j} + c)$ διαιρείται από το $\gamma(x)$, τότε θα έπρεπε το $x^{i-j} + c$ να διαιρείτο από το $\gamma(x)$, άτοπο.

□

Όπως παρατηρούμε το αποτέλεσμα που βρήκαμε για την ελάχιστη απόσταση του κώδικα στο Παράδειγμα 2.6.6, *συνάδει* με την προηγούμενη πρόταση, καθότι το πολυώνυμο γεννήτορας $\gamma(x) = 1+x+x^3$ δεν διαιρεί κανένα από τα πολυώνυμα $x^4 + 1$ και $x^5 + 1$.

Τώρα θα αποδείξουμε (δίνοντας ένα παράδειγμα) ότι ο δυϊκός κώδικας ενός πολυωνυμικού κώδικα δεν είναι κατ' ανάγκη πολυωνυμικός κώδικας.

Παράδειγμα 2.6.10. Έστω ο δυαδικός πολυωνυμικός κώδικας $\mathcal{C}$ μήκους 7 με γεννήτορα πολυώνυμο το $\gamma(x) = 1 + x + x^3$. Ένας γεννήτορας πίνακας είναι ο

$$\mathrm{G} = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}.$$

Ως γνωστόν ένα στοιχείο $\mathbf{x} = x_1\, x_2\, x_3\, x_4\, x_5\, x_6\, x_7$ ανήκει στον δυϊκό κώδικα αν και μόνο αν $\mathrm{G}\mathbf{x}^t = \mathbf{0}$. Από την τελευταία σχέση έπεται ότι ένας πίνακας ελέγχου ισοτιμίας για τον $\mathcal{C}$ είναι ο $\mathrm{P} = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}$ (γιατί;). Επομένως ο δυϊκός κώδικας $\mathcal{C}^\perp$ έχει ως γεννήτορα πίνακα τον πίνακα P. Αν ο $\mathcal{C}^\perp$ ήταν πολυωνυμικός, θα είχε ένα γεννήτορα πολυώνυμο έστω $g(x) = 1 + c_1x + c_2x^2 + c_3x^3 + c_4x^4$. Για κάθε πολύωνυμο $a_0 + a_1x + a_2x^2$ με συντελεστές από το $\mathbb{Z}_2$, οι συντελεστές του γινομένου $(a_0 + a_1x + a_2x^2)g(x)$ αποτελούν μια (κωδικο)λέξη του $\mathcal{C}^\perp$, την $(a_0\, a_1\, a_2)\mathrm{P}$. Εκτελούμε τον παραπάνω πολλαπλασιασμό πολυωνύμων, τον πολλαπλασιασμό $(a_0\, a_1\, a_2)\mathrm{P}$ και συγκρίνουμε τα δύο αποτελέσματα. Πρέπει να ισχύει

$$\begin{aligned} a_0 &= a_0 \\ a_0c_1 + a_1 &= a_1 \\ a_0c_2 + a_1c_1 + a_2 &= a_2 \\ a_0c_3 + a_1c_2 + a_2c_1 &= a_0 + a_1 \\ a_0c_4 + a_1c_3 + a_2c_2 &= a_1 + a_2 \\ a_1c_4 + a_2c_3 &= a_0 + a_1 + a_2 \\ a_2c_4 &= a_0 + a_2 \end{aligned}$$

Από την δεύτερη και τρίτη ισότητα έπεται ότι τα c_1 και c_2 πρέπει να είναι ίσα με μηδέν, οπότε η τέταρτη ισότητα γίνεται $a_0c_3 = a_0 + a_1$. Η ισότητα αυτή θα πρέπει να ισχύει για κάθε a_0, $a_1 \in \mathbb{Z}_2$. Αυτό όμως είναι αδύνατον (γιατί;). Άρα ο δυϊκός κώδικας $\mathcal{C}^\perp$ δεν είναι πολυωνυμικός.

2.6.2 Κυκλικοί κώδικες

Μια ειδική, αλλά η πλέον ενδιαφέρουσα, κατηγορία πολυωνυμικών κωδίκων είναι οι κυκλικοί κώδικες. Οι κυκλικοί κώδικες έχουν πλούσια αλγεβρική δομή, η οποία τους καθιστά αποτελεσματικούς και όπως θα δούμε στα επόμενα οι πλέον σημαντικές οικογένειες κωδίκων περιλαμβάνουν κώδικες ισοδύναμους με κυκλικούς κώδικες.

Ορισμός 2.6.11. *Ένας γραμμικός κώδικας $\mathcal{C}$ μήκους n θα λέγεται κυκλικός αν για κάθε (κωδικο)λέξη $\mathbf{c} = c_0\, c_1 \cdots c_{n-1}$ η λέξη που προκύπτει με*

μια κυκλική μετάθεση των χαρακτήρων της κατά ένα βήμα, δηλαδή η λέξη $c_{n-1}\, c_0\, c_1 \cdots c_{n-2}$, *είναι και αυτή στοιχείο του κώδικα.*

Από τον ορισμό έπεται αμέσως ότι για κάθε $1 \leq k \leq n-1$ η λέξη $c_k \cdots c_{n-1}\, c_0\, c_1 \cdots c_{k-1}$ είναι και αυτή στοιχείο του κώδικα.

Παραδείγματα 2.6.12. 1. Οι ακραίες περιπτώσεις του μηδενικού κώδικα και του κώδικα που είναι όλος ο διανυσματικός χώρος $\mathbb{F}_p^n$, αποτελούν τετριμμένα παραδείγματα κυκλικών κωδίκων.

2. Προφανώς ο επαναληπτικός κώδικας $\mathcal{R}_p(k) = \{ \underbrace{00\cdots0}_{k-\text{φορές}}, \underbrace{11\cdots1}_{k-\text{φορές}}, \ldots, \underbrace{p-1\, p-1 \cdots p-1}_{k-\text{φορές}} \}$ είναι κυκλικός.

3. Ο δυαδικός κώδικας $\mathcal{C} = \{\, 000,\, 101,\, 011,\, 110 \,\}$ προφανώς είναι κυκλικός κώδικας.

4. Ο δυαδικός πολυωνυμικός κώδικας $[7,\, 4,\, 3]$ $\mathcal{C}$ του Παραδείγματος 2.6.10 με γεννήτορα πίνακα $\mathrm{G} = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}$ είναι εύκολο να διαπιστώσουμε ότι είναι ένας κυκλικός κώδικας.

5. Ο δυαδικός κώδικας $\mathcal{C} = \{\, 0000,\, 1001,\, 0110,\, 1111 \,\}$ δεν είναι κυκλικός (γιατί;). Αντιμεταθέτοντας όμως τους χαρακτήρες της τρίτης και τέταρτης θέσης λαμβάνουμε τον κώδικα $\mathcal{D} = \{\, 0000,\, 1010,\, 0101,\, 1111 \,\}$, ο οποίος είναι κυκλικός. Δηλαδή υπάρχουν μη κυκλικοί γραμμικοί κώδικες οι οποίοι είναι ισοδύναμοι με κυκλικούς κώδικες.

6. Ο $p-$αδικός κώδικας $\mathcal{E}_n$ που αποτελείται από όλες τις λέξεις μήκους n με άθροισμα χαρακτήρων ίσον με μηδέν (βλέπε Παράδειγμα $2.1.2_5$) είναι ένας κυκλικός κώδικας (γιατί;)

Όπως και στην προηγούμενη παράγραφο με $\mathbb{F}$ θα συμβολίζουμε το σώμα $\mathbb{F}_p$, όπου p είναι ένας πρώτος αριθμός. Επίσης σύμφωνα με την Πρόταση 2.6.1 θα ταυτίζουμε γραμμικούς κώδικες μήκους n με υποχώρους του $\mathbb{F}_{n-1}[x]$.

Έστω τώρα ένας γραμμικός κώδικας $\mathcal{C}$ μήκους n και $a_0\, a_1 \cdots a_{n-1}$ ένα στοιχείο του. Σύμφωνα με τα προηγούμενα έχουμε το πολυώνυμο $a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}$. Πολλαπλασιάζοντας το πολυώνυμο αυτό με x έχουμε $x(a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}) = a_0 x + a_1 x^2 + \cdots + a_{n-1}x^n$. Αν στην τελευταία σχέση *αντικαταστήσουμε* το x^n με το 1, έχουμε το πολυώνυμο $a_{n-1} + a_0 x + a_1 x^2 +$

$\cdots + a_{n-2}x^{n-1}$, οπότε παρατηρούμε ότι οι συντελεστές $a_{n-1}\,a_0\,a_1\,\cdots\,a_{n-2}$ του τελευταίου πολυωνύμου αντιστοιχούν σε μια κυκλική μετάθεση κατά μια θέση των χαρακτήρων της (κωδικο)λέξης $a_0\,a_1\,\cdots\,a_{n-1}$. Όμοια μια κυκλική μετάθεση κατά k το πλήθος θέσεις *αντιστοιχεί* σε πολλαπλασιασμό του πολυωνύμου $a_0 + a_1x + \cdots + a_{n-1}x^{n-1}$ με x^k και *αντικατάσταση* του x^n με το 1. Επομένως είναι φανερό ότι οι κυκλικοί κώδικες έχουν σχέση με την *αντικατάσταση* του x^n με το 1. Η διαδικασία όμως αυτή δεν είναι τίποτε άλλο από να διαιρέσουμε ένα πολυωνύμο με το x^n-1 και να κρατήσουμε το υπόλοιπο της διαίρεσης. Πράγματι, έστω $\phi(x) \in \mathbb{F}[x]$, από την ταυτότητα της διαίρεσης πολυωνύμων έχουμε ότι υπάρχουν (μοναδικά) $\pi(x)$, $\upsilon(x) \in \mathbb{F}[x]$ τέτοια ώστε $\phi(x) = \pi(x)\cdot(x^n-1)+\upsilon(x)$ και $\upsilon(x) = 0$ ή $deg(\upsilon(x)) \leq n-1$. Οπότε για $x^n = 1$ στη θέση του $\phi(x)$ έχουμε το υπόλοιπο $\upsilon(x)$.

Προσοχή! Όταν λέμε αντικαθιστούμε το x^n με το 1, εννοούμε ότι αντικαθιστούμε το πολυώνυμο x^n με το σταθερό πολυώνυμο 1 και **όχι** το x λαμβάνει την τιμή 1.

Έστω $\tau_1(x), \tau_2(x) \in \mathbb{F}_{n-1}[x]$. Από την ταυτότητα της διαίρεσης πολυωνύμων έχουμε ότι υπάρχουν (μοναδικά) $\pi(x), \upsilon(x) \in \mathbb{F}_{n-1}[x]$ τέτοια ώστε $\tau_1(x)\cdot\tau_2(x) = \pi(x)\cdot(x^n-1)+\upsilon(x)$ και $\upsilon(x) = 0$ ή $deg(\upsilon(x)) \leq n-1$. Στο σύνολο $\mathbb{F}_{n-1}[x]$ ορίζουμε έναν *πολλαπλασιασμό* πολυωνύμων ως εξής:

$$\tau_1(x) \odot \tau_2(x) =: \upsilon(x)\,,$$

όπου $\upsilon(x)$ είναι το υπόλοιπο της προηγούμενης διαίρεσης. Ο πολλαπλασιασμός αυτός θα λέγεται **πολλαπλασιασμός** $\bmod(x^n-1)$.

Για παράδειγμα, αν x^3+x+1, $x^2+x+1 \in \mathbb{Z}_2[x]$, τότε $(x^3+x+1)\cdot(x^2+x+1) = x^5+x+1 = (x+1)\cdot(x^4+1)+x \in Z_2[x]$, οπότε $(x^3+x+1)\odot(x^2+x+1) = x$.

Δεν είναι δύσκολο να δούμε ότι το σύνολο $\mathbb{F}_{n-1}[x]$ με πράξεις την πρόσθεση πολυωνύμων και τον πολλαπλασιασμό $\bmod(x^n-1)$ είναι ένας μεταθετικός δακτύλιος με μονάδα. (Ως άσκηση μπορείτε να ελέγξετε την προσεταιριστική ιδιότητα του πολλαπλασιασμού.)

Σημείωση: Στα επόμενα πολλές φορές, όταν δεν υπάρχει κίνδυνος σύγχυσης, τον πολλαπλασιασμό $\bmod(x^n-1)$ θα τον συμβολίζουμε $\tau_1(x)\cdot\tau_2(x)$, όπως τον συνήθη πολλαπλασιασμό πολυωνύμων.

Χρησιμοποιώντας την έννοια του ιδεώδους και την έννοια του δακτυλίου πηλίκο μπορούμε να περιγράψουμε κομψά την παραπάνω διαδικασία και τους κυκλικούς κώδικες.

Έστω $\mathbb{F}[x]$ ο δακτύλιος όλων των πολυωνύμων με συντελεστές από το σώμα $\mathbb{F}$ και $\langle x^n-1\rangle$ το (κύριο) ιδεώδες το παραγόμενο από το πολυώνυμο x^n-1. Δηλαδή $\langle x^n-1\rangle = \{\,\sigma(x)\cdot(x^n-1) \mid \sigma(x) \in \mathbb{F}[x]\,\}$. Ο δακτύλιος πηλίκο

$\mathbb{F}[x]/\langle x^n-1\rangle$ αποτελείται από όλα τα σύμπλοκα της μορφής $\tau(x)+\langle x^n-1\rangle$ με $\tau(x)\in\mathbb{F}[x]$. Δύο στοιχεία $\tau_1(x)+\langle x^n-1\rangle$ και $\tau_2(x)+\langle x^n-1\rangle$ του $\mathbb{F}[x]/\langle x^n-1\rangle$ είναι ίσα αν και μόνο αν η διαφορά $\tau_1(x)-\tau_2(x)$ ανήκει στο ιδεώδες $\langle x^n-1\rangle$ ή ισοδύναμα διαιρείται από το x^n-1.

Πρόταση 2.6.13. *Η απεικόνιση $\varphi:\mathbb{F}_{n-1}[x]\longrightarrow\mathbb{F}[x]/\langle x^n-1\rangle$ με $\varphi(\tau(x))=\tau(x)+\langle x^n-1\rangle$ είναι ένας ισομορφισμός δακτυλίων.*

Απόδειξη. Ο έλεγχος ότι η απεικόνιση φ πληροί τις παραπάνω ιδιότητες είναι απλός και αφίνεται ως άσκηση.

□

Ο προηγούμενος ισομορφισμός μας επιτρέπει να *ταυτίσουμε* τους δύο δακτυλίους και στα επόμενα θα τους συμβολίζουμε χωρίς διάκριση με $\mathcal{R}_n$ ($\mathcal{R}_n:=\mathbb{F}_{n-1}[x]\cong_\varphi\mathbb{F}[x]/\langle x^n-1\rangle$).

Έστω τώρα ένας κώδικας μήκους n, δηλαδή $\mathcal{C}\subseteq\mathbb{F}^n$. Από την Πρόταση 2.6.1 και την προηγούμενη πρόταση, επειδή οι απεικονίσεις φ και ψ^{-1} είναι 1 - 1, στα επόμενα θα μπορούμε να ταυτίσουμε τον κώδικα $\mathcal{C}$ με την εικόνα του και να τον θεωρούμε ως υποσύνολο του $\mathcal{R}_n$.

Θεώρημα 2.6.14. *Ένας κώδικας $\mathcal{C}$ είναι κυκλικός αν και μόνο αν είναι ένα ιδεώδες του δακτυλίου $\mathcal{R}_n$.*

Απόδειξη. Υποθέτουμε ότι ο κώδικας είναι κυκλικός. Τότε για
$\alpha_1(x),\alpha_2(x)\in\mathcal{C}\subseteq\mathcal{R}_n$ έχουμε ότι
(i) $\quad\alpha_1(x)-\alpha_2(x)\in\mathcal{C}$, αφού ο $\mathcal{C}$ είναι γραμμικός.
Έστω τώρα $\alpha(x)\in\mathcal{C}$ και $\tau(x)=r_0+r_1x+\cdots+r_kx^k\in\mathcal{R}_n$. Από τα προηγούμενα έχουμε ότι ο πολλαπλασιασμός του $\alpha(x)$ με x αντιστοιχεί με μια κυκλική μετάθεση κατά μια θέση, δηλαδή $x\cdot\alpha(x)\in\mathcal{C}$, αφού ο $\mathcal{C}$ είναι κυκλικός, όμοια $x^2\cdot\alpha(x),\ldots,x^k\cdot\alpha(x)\in\mathcal{C}$. Επομένως
(ii) $\quad\tau(x)\cdot\alpha(x)=r_0\alpha(x)+r_1x\alpha(x)+\cdots+r_kx^k\alpha(x)\in\mathcal{C}$.
(Δεν ξεχνάμε ο πολλαπλασιασμός πολυωνύμων είναι $\bmod(x^n-1)$.)
Από τις σχέσεις (i)και (ii) έπεται ότι ο $\mathcal{C}$ είναι ένα ιδεώδες του $\mathcal{R}_n$.

Αντίστροφα, υποθέτουμε ότι ο κώδικας $\mathcal{C}$ είναι ένα ιδεώδες του $\mathcal{R}_n$, δηλαδή ισχύουν οι (i) και (ii). Λαμβάνοντας στη θέση του $\tau(x)$ στη σχέση (ii) ένα σταθερό πολυώνυμο, αποδεικνύουμε (σε συνδυασμό με τη σχέση (i)) ότι ο κώδικας είναι γραμμικός. Αν στη θέση του $\tau(x)$ στη σχέση (ii) λάβουμε το πολυώνυμο x , αποδεικνύουμε ότι ο κώδικας είναι κυκλικός. □

Από το προηγούμενο θεώρημα έπεται ότι για να υπολογίσουμε όλους τους κυκλικούς κώδικες μήκους n (πρέπει και) αρκεί να υπολογίσουμε όλα τα ιδεώδη του δακτυλίου $\mathcal{R}_n$.

Ένας τρόπος κατασκεύης κυκλικών κωδίκων (και όπως θα δούμε στα επόμενα ο μοναδικός) είναι να θεωρήσουμε τα κύρια ιδεώδη του δακτυλίου $\mathcal{R}_n$. Έστω $p(x) \in \mathcal{R}_n$, τότε το (κύριο) ιδεώδες το παραγόμενο από το $p(x)$ αποτελείται από όλα τα πολλαπλάσια του $p(x)$, δηλαδή $\langle\, p(x) \,\rangle = \{\, r(x) \cdot p(x) \mid r(x) \in \mathcal{R}_n \,\}$. Σύμφωνα με τα προηγούμενα το $\mathcal{C} = \langle\, p(x) \,\rangle = \{\, r(x) \cdot p(x) \mid r(x) \in \mathcal{R}_n \,\}$ είναι ένας κυκλικός κώδικας που παράγεται από το πολυώνυμο $p(x)$.

Παράδειγμα 2.6.15. Έστω ο δυαδικός κυκλικός κώδικας $\mathcal{C} = \langle\, 1 + x^2 \,\rangle = \{\, r(x) \cdot (1 + x^2) \mid r(x) \in \mathcal{R}_3 \,\}$. Το $\mathcal{R}_3$ αποτελείται από οκτώ στοιχεία (τα δυνατά υπόλοιπα της διαίρεσης ενός πολυωνύμου $r(x) \in \mathbb{Z}_2[x]$ με το $x^3 - 1$), δηλαδή $\mathcal{R}_3 = \{\, 0,\, 1,\, x,\, 1 + x,\, x^2,\, 1 + x^2,\, x + x^2,\, 1 + x + x^2 \,\}$. Οπότε κάνοντας τους πολλαπλασιασμούς $(\mathrm{mod}(x^3 - 1))$ βρίσκουμε ότι $\mathcal{C} = \{\, 0,\, 1 + x,\, 1 + x^2,\, x + x^2 \,\}$. Δηλαδή $\mathcal{C} = \{\, 000,\, 110,\, 101,\, 011 \,\}$, ο κώδικας του Παραδείγματος $2.6.12_2$.

Θεώρημα 2.6.16. *Έστω $\mathcal{C}$ ένας μη μηδενικός κυκλικός κώδικας μήκους n. Τότε υπάρχει μοναδικό μονικό πολυώνυμο $\gamma(x) \in \mathcal{R}_n$ ελαχίστου βαθμού έτσι ώστε $\mathcal{C} = \langle \gamma(x) \rangle$. Επιπλέον το πολυώνυμο $\gamma(x)$ διαιρεί το πολυώνυμο $x^n - 1$.*

Απόδειξη. Έστω $\alpha(x), \beta(x) \in \mathcal{C}$ δύο διαφορετικά μονικά πολυώνυμα με τον μικρότερο δυνατόν βαθμό. Ο κώδικας είναι γραμμικός, επομένως η διαφορά $\alpha(x) - \beta(x) \in \mathcal{C}$ και έχει βαθμό μικρότερο από τον βαθμό των $\alpha(x)$ και $\beta(x)$. Πολλαπλασιάζοντας το $\alpha(x) - \beta(x)$ με τον αντίστροφο συντελεστή του μεγιστοβαθμίου όρου έχουμε ένα πολυώνυμο, το οποίο ανήκει στον κώδικα $\mathcal{C}$, είναι μονικό και έχει βαθμό μικρότερο από τον βαθμό των $\alpha(x)$ και $\beta(x)$, άτοπο.

Έστω $\gamma(x)$ το μοναδικό μονικό πολυώνυμο ελαχίστου βαθμού στον $\mathcal{C}$ και $\alpha(x) \in \mathcal{C}$. Από την ταυτότητα της διαίρεσης στο $\mathbb{F}[x]$ έχουμε ότι υπάρχουν πολυώνυμα $\pi(x), \upsilon(x) \in \mathbb{F}[x]$ τέτοια ώστε $\alpha(x) = \pi(x) \cdot \gamma(x) + \upsilon(x)$ με $\upsilon(x) = 0$ ή $deg(\upsilon(x)) < deg(\gamma(x))$. Από το Θεώρημα 2.6.14 έπεται ότι $\upsilon(x) = \alpha(x) - \pi(x) \cdot \gamma(x) \in \mathcal{C}$. Επειδή το $\gamma(x)$ είναι ελαχίστου βαθμού (και ο κώδικας γραμμικός), έπεται ότι $\upsilon(x) = 0$ και επομένως $\mathcal{C} = \langle \gamma(x) \rangle$.

Επίσης από την ταυτότητα της διαίρεσης στο $\mathbb{F}[x]$ έχουμε ότι υπάρχουν πολυώνυμα $\pi_1(x), \upsilon_1(x) \in \mathbb{F}[x]$ τέτοια ώστε $x^n - 1 = \pi_1(x) \cdot \gamma(x) + \upsilon_1(x)$ με $\upsilon_1(x) = 0$ ή $deg(\upsilon_1(x)) < deg(\gamma(x))$. Αλλά $x^n - 1 = 0 \in \mathcal{R}_n$, επομένως $\upsilon_1(x) = -\pi_1(x) \cdot \gamma(x) \in \mathcal{C} = \langle \gamma(x) \rangle$. Άρα $\upsilon_1(x) = 0$.

□

Παρατήρηση 2.6.17. Για όσους είναι εξοικειωμένοι με τις στοιχειώδεις ιδιότητες των ιδεωδών και του δακτυλίου πηλίκο, η προηγούμενη πρόταση είναι μια μερική περίπτωση της εξής γενικής πρότασης: Έστω $\mathbb{F}$ ένα σώμα. Κάθε ιδεώδες του δακτυλίου $\mathbb{F}[x]$ είναι κύριο. Αν $I = \langle r(x) \rangle$, $J = \langle s(x) \rangle$ είναι ιδεώδη του $\mathbb{F}[x]$ με $I \subseteq J$, τότε το πολυώνυμο $s(x)$ διαιρεί το $r(x)$. Επιπλέον κάθε ιδεώδες

του δακτυλίου $\mathbb{F}[x]/I$ είναι της μορφής J/I, όπου J είναι ένα ιδεώδες του $\mathbb{F}[x]$ με $I \subseteq J$.
Η απόδειξη είναι (ακριβώς) η ίδια με την απόδειξη της προηγούμενης πρότασης.

Το μοναδικό μονικό πολυώνυμο $\gamma(x)$, που υπάρχει από το προηγούμενο θεώρημα, θα λέγεται το **πολυώνυμο γεννήτορας** του κώδικα $\mathcal{C}$.

Εδώ θα θέλαμε να επισημάνουμε ότι ένας κυκλικός κώδικας $\mathcal{C}$ ως κύριο ιδεώδες του δακτυλίου $\mathcal{R}_n$ ενδέχεται να παράγεται από περισσότερα του ενός πολυωνύμων, δηλαδή να υπάρχουν περισσότερα του ενός πολυώνυμα $f(x) \in \mathcal{R}_n$ έτσι ώστε $\mathcal{C} = \langle f(x) \rangle$, **αλλά** υπάρχει μόνο ένα πολυώνυμο γεννήτορας.

Στο προηγούμενο παράδειγμα ο κώδικας $\mathcal{C} = \langle 1 + x^2 \rangle$ παράγεται μεν από το πολυώνυμο $1 + x^2$, αλλά το πολυώνυμο γεννήτορας είναι το $1 + x$ (γιατί;)

Θεώρημα 2.6.18. *Ένα μονικό πολυώνυμο $g(x) \in \mathcal{R}_n$ είναι το πολυώνυμο γεννήτορας ενός κυκλικού κώδικα $\mathcal{C} \subseteq \mathcal{R}_n$ αν και μόνο αν το $g(x)$ διαιρεί το $x^n - 1$.*

Απόδειξη. Η μια κατεύθυνση έχει ήδη αποδειχθεί στο Θεώρημα 2.6.16.

Υποθέτουμε ότι το $g(x)$ διαιρεί το $x^n - 1$, δηλαδή $x^n - 1 = t(x) \cdot g(x)$. Έστω ο κυκλικός κώδικας $\mathcal{C} = \langle g(x) \rangle$. Από το προηγούμενο θεώρημα υπάρχει το πολυώνυμο γεννήτορας, έστω $\gamma(x)$, του $\mathcal{C}$. Υποθέτουμε ότι $\gamma(x) \neq g(x)$. Το $\gamma(x)$ είναι το πολυώνυμο γεννήτορας και το $g(x)$ μονικό, επομένως ο βαθμός του είναι (γνήσια) μικρότερος από τον βαθμό του $g(x)$. Επειδή $\gamma(x) \in \mathcal{C} = \langle g(x) \rangle$, υπάρχει πολυώνυμο $r(x)$ έτσι ώστε $\gamma(x) = g(x) \cdot r(x)$. Ο τελευταίος πολλαπλασιασμός είναι $\bmod(x^n - 1)$, αυτό σημαίνει ότι υπάρχει πολυώνυμο $\pi(x)$ έτσι ώστε $\gamma(x) = g(x) \cdot r(x) + \pi(x) \cdot (x^n - 1)$. Πολλαπλασιάζοντας την τελευταια σχέση με $t(x)$ έχουμε $t(x) \cdot \gamma(x) = t(x) \cdot (g(x) \cdot r(x) + \pi(x) \cdot (x^n - 1)) = (t(x) \cdot g(x)) \cdot r(x) + t(x) \cdot \pi(x) \cdot (x^n - 1)$. Αλλά $x^n - 1 = t(x) \cdot g(x)$, οπότε, αντικαθιστώντας στην τελευταία σχέση, έχουμε $t(x) \cdot \gamma(x) = (x^n - 1) \cdot r(x) + t(x) \cdot \pi(x) \cdot (x^n - 1) = (x^n - 1) \cdot (r(x) + t(x) \cdot \pi(x))$. Από την τελευταία σχέση έχουμε ότι ο βαθμός του γινομένου $t(x) \cdot \gamma(x)$ είναι μεγαλύτερος ή ίσος του γινομένου $t(x) \cdot g(x)$. Αυτό έρχεται σε αντίφαση με το ότι ο βαθμός του $\gamma(x)$ είναι (γνήσια) μικρότερος από τον βαθμό του $g(x)$. Άρα $g(x) = \gamma(x)$. □

Από τα δύο προηγούμενα θεωρήματα είναι φανερό ότι το πρόβλημα του προσδιορισμού όλων των κυκλικών κωδικών μήκους n επί ενός πεπερασμένου σώματος $\mathbb{F}_p$ είναι ισοδύναμο με τον προσδιορισμό της ανάλυσης του πολυωνύμου $x^n - 1$ σε γινόμενο (αναγώγων) παραγόντων επί του $\mathbb{F}_p$.

Εδώ πρέπει να επισημάνουμε ότι αν $n = p^r \cdot m$ με p να μην διαιρεί τον m, τότε $x^n - 1 = (x^m - 1)^{p^r}$. Επομένως το πρόβλημα ανάγεται στην παραγοντοποίηση πολυωνύμων της μορφής $x^n - 1$ με p να μην διαιρεί τον n. [4]

[4] Για το λόγο αυτό θα υποθέτουμε σιωπηλά (χωρίς βλάβη της γενικότητας) ότι ο p δεν διαιρεί τον n.

Παράδειγμα 2.6.19. Έστω το πολυώνυμο $x^3-1 \in \mathbb{Z}_2[x]$. Προφανώς $x^3-1 = (x+1)(x^2+x+1)$. Επομένως υπάρχουν τέσσερεις διαιρέτες του x^3-1, οι 1, $x+1$, x^2+x+1 και $(x+1)(x^2+x+1) = x^3-1$. Οι αντίστοιχοι κυκλικοί κώδικες είναι οι εξής:
$\langle 1 \rangle = \mathcal{R}_3 = \{\, 000,\, 001,\, 010,\, 011,\, 100,\, 101,\, 110,\, 111 \,\}$
$\langle x+1 \rangle = \{\, 0,\, 1+x,\, x+x^2,\, 1+x^2 \,\} = \{\, 000,\, 110,\, 011,\, 101 \,\}$
$\langle x^2+x+1 \rangle = \{\, 0,\, 1+x+x^2 \,\} = \{\, 000,\, 111 \,\}$
$\langle x^3-1 \rangle = \{\, 0 \,\} = \{\, 000 \,\}$

Από το Θεώρημα 2.6.16 έχουμε ότι ένας κυκλικός κώδικας είναι πολυωνυμικός, επομένως μπορούμε να αποδείξουμε μια πρόταση ανάλογη με την Πρόταση 2.6.7.

Πρόταση 2.6.20. *Έστω $\mathcal{C} \subseteq \mathcal{R}_n$ ένας κυκλικός κώδικας με γεννήτορα πολυώνυμο $\gamma(x) = c_0 + c_1x + \cdots + c_kx^k$. Τότε $c_0 \neq 0$, η διάστασή του είναι ίση με $n-k$ και ένας γεννήτορας πίνακας είναι ο $(n-k) \times n$ πίνακας*

$$\mathrm{G} = \begin{pmatrix} c_0 & c_1 & \cdots & c_k & 0 & 0 & \cdots & 0 \\ 0 & c_0 & \cdots & c_{k-1} & c_k & 0 & \cdots & 0 \\ \vdots & \vdots & \cdots & \vdots & \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & 0 & c_0 & c_1 & \cdots & c_k \end{pmatrix}$$

Απόδειξη. Υποθέτουμε ότι $c_0 = 0$. Τότε $x^{n-1}\gamma(x) = x^{-1}\gamma(x)$ ανήκει στον κώδικα και έχει βαθμό ίσον με $k-1$, μικρότερο από τον βαθμό του $\gamma(x)$, άτοπο.

Η απόδειξη τώρα είναι παρόμοια με την απόδειξη της Πρότασης 2.6.7.

□

Παρατηρήσεις 2.6.21.

1. Στην περίπτωση των πολυωνυμικών κωδίκων είχαμε δεί ότι μπορούμε να υποθέσουμε ότι ο σταθερός όρος του γεννήτορα πολυωνύμου είναι διάφορος του μηδενός (βλέπε Παρατήρηση 2.6.5 $_5$). Στους κυκλικούς κώδικες αποδείξαμε ότι ο σταθερός όρος του γεννήτορα πολυωνύμου είναι διάφορος του μηδενός.

2. Δεν είναι δύσκολο να δούμε ότι το σύνολο
$\{\, \gamma(x),\, x\gamma(x),\, x^2\gamma(x),\, \ldots,\, x^{n-k-1}\gamma(x) \,\}$ είναι μια βάση του κώδικα $\mathcal{C}$ (γιατί;), επομένως έχουμε μια άλλη απόδειξη της προηγουμένης πρότασης.

Παράδειγμα 2.6.22. Έστω το πολυώνυμο $x^4-1 \in \mathbb{Z}_3[x]$. Προφανώς $x^4-1 = (x-1)(x+1)(x^2+1)$. Επομένως υπάρχουν οκτώ διαιρέτες του x^4-1, οι 1, $x-1$, $x+1$, x^2+1, $(x-1)(x+1)$, $(x-1)(x^2+1)$, $(x+1)(x^2+1)$, x^4-1. Οι γεννήτορες πίνακες των αντίστοιχων κυκλικών κωδίκων είναι κατά σειρά οι εξής:

$$I_4,\quad \begin{pmatrix} -1 & 1 & 0 & 0 \\ 0 & -1 & 1 & 0 \\ 0 & 0 & -1 & 1 \end{pmatrix},\quad \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix},\quad \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}$$
$$\begin{pmatrix} -1 & 0 & 1 & 0 \\ 0 & -1 & 0 & 1 \end{pmatrix},\quad \begin{pmatrix} -1 & 1 & -1 & 1 \end{pmatrix},\quad \begin{pmatrix} 1 & 1 & 1 & 1 \end{pmatrix},\quad \begin{pmatrix} 0 & 0 & 0 & 0 \end{pmatrix}$$

Εδώ θα πρέπει να αναφέρουμε ότι κάθε πολυωνυμικός κώδικας δεν είναι κατ' ανάγκη κυκλικός κώδικας. Πράγματι, στο παράδειγμα 2.6.6 ο δυαδικός πολυωνυμικός κώδικας μήκους 6 με γεννήτορα πολυώνυμο $1+x+x^3$ δεν είναι κυκλικός αφού το $1\,1\,1\,0\,0\,1$ είναι (κωδικο)λέξη, ενώ το $1\,1\,1\,1\,0\,0$ δεν είναι.

Έστω $\mathcal{C}_1, \mathcal{C}_2 \in \mathcal{R}_n$ δύο κυκλικοί κώδικες, τότε ορίζουμε το άθροισμά τους ως εξής: $\mathcal{C}_1 + \mathcal{C}_2 = \{\, \mathbf{c}_1 + \mathbf{c}_2 \mid \mathbf{c}_1 \in \mathcal{C}_1,\, \mathbf{c}_2 \in \mathcal{C}_2 \,\}$. [5]

Πρόταση 2.6.23. *Έστω $\mathcal{C}_1, \mathcal{C}_2 \subseteq \mathcal{R}_n$ κυκλικοί κώδικες με γεννήτορες πολυώνυμα $\gamma_1(x)$ και $\gamma_2(x)$ αντίστοιχα, τότε έχουμε.*

1. *$\mathcal{C}_1 \subseteq \mathcal{C}_2$ αν και μόνο αν το $\gamma_2(x)$ διαιρεί το $\gamma_1(x)$.*
2. *Η τομή $\mathcal{C}_1 \cap \mathcal{C}_2$ είναι κυκλικός κώδικας με γεννήτορα πολυώνυμο το ελάχιστο κοινό πολλαπλάσιο των $\gamma_1(x)$ και $\gamma_2(x)$.*
3. *Το άθροισμα $\mathcal{C}_1 + \mathcal{C}_2$ είναι κυκλικός κώδικας με γεννήτορα πολυώνυμο τον μέγιστο κοινό διαιρέτη των $\gamma_1(x)$ και $\gamma_2(x)$.*

Απόδειξη. Ως γνωστόν το άθροισμα και η τομή ιδεωδών είναι ιδεώδες, οπότε η απόδειξη έπεται από το θεώρημα 2.6.14, με τις λεπτομέρειες να αφίνονται ως άσκηση.

□

Υποθέτουμε, ότι $x^n - 1 = \prod_{i=1}^{k} m_i(x)$ είναι η ανάλυση του σε γινόμενο μονικών αναγώγων πολυωνύμων επί του σώματος $\mathbb{F}_p$. Για κάθε $i = 1, \ldots, k$ έστω ο κυκλικός κώδικας $\mathcal{C}_i$ με γεννήτορα πολυώνυμο το πολυώνυμο $m_i(x)$. Από την προηγούμενη πρόταση έχουμε ότι δεν υπάρχει κυκλικός κώδικας (εκτός από τον ίδιο τον $\mathcal{R}_n$), ο οποίος να περιέχει τον κώδικα $\mathcal{C}_i$. Με αυτή την έννοια οι κώδικες $\mathcal{C}_i$ είναι *μέγιστοι*. Προφανώς κάθε κυκλικός κώδικας με γεννήτορα πολυώνυμο $\gamma(x)$ περιέχεται στους αντίστοιχους μέγιστους κυκλικούς κώδικες με πολυώνυμα γεννήτορες ανάγωγους παράγοντες του $\gamma(x)$.

Δυϊκά έστω $\mu_i(x) = \frac{x^n-1}{m_i(x)}$ και $\mathcal{D}_i$ οι κυκλικοί κώδικες με πολυώνυμα γεννήτορες αντίστοιχα τα πολυώνυμα $\mu_i(x)$, πάλι από την προηγούμενη πρόταση έχουμε

[5] Το άθροισμα κυκλικών κωδίκων δεν είναι τίποτε άλλο από το γνωστό άθροισμα διανυσματικών υποχώρων.

ότι δεν υπάρχει κυκλικός κώδικας (εκτός από τον μηδενικό) που να περιέχεται στους κώδικες $\mathcal{D}_i$. Με αυτή την έννοια οι κώδικες αυτοί είναι *ελάχιστοι*. Προφανώς κάθε ελάχιστος κώδικας $\mathcal{D}_i$ περιέχεται σε όλους τους κυκλικούς κώδικες των οποίων το ελάχιστο πολυώνυμο δεν διαιρείται από το πολυώνυμο $m_i(x)$.

Το πολυώνυμο ελέγχου ενός κυκλικού κώδικα

Έστω $\mathcal{C}$ ένας $[n, k]$ κυκλικός κώδικας με γεννήτορα πολυώνυμο $\gamma(x)$, από το Θεώρημα 2.6.16 υπάρχει (μοναδικό) μονικό πολυώνυμο $\delta(x)$ έτσι ώστε $x^n - 1 = \gamma(x) \cdot \delta(x)$. Από την Πρόταση 2.6.20 έχουμε ότι ο βαθμός του $\gamma(x)$ είναι ίσος με $n - k$, άρα ο βαθμός του $\delta(x)$ είναι ίσος με k.

Το πολυώνυμο $\delta(x)$ θα λέγεται **πολυώνυμο ελέγχου** για τον κυκλικό κώδικα $\mathcal{C}$.

Η έννοια του πολυωνύμου ελέγχου στους κυκλικούς κώδικες είναι *παράλληλη* με την έννοια του πίνακα ελέγχου ισοτιμίας, όπως θα δούμε στα επόμενα.

Θεώρημα 2.6.24. *Έστω $\mathcal{C} \subseteq \mathcal{R}_n$ ένας κυκλικός κώδικας με γεννήτορα πολυώνυμο $\gamma(x)$ και πολυώνυμο ελέγχου $\delta(x)$. Τότε μπορούμε να περιγράψουμε τα στοιχεία του $\mathcal{C}$ ως εξής: Ένα $c(x) \in \mathcal{R}_n$ ανήκει στον κώδικα $\mathcal{C}$ αν και μόνο αν $c(x) \cdot \delta(x) = 0$.*

(Υπενθυμίζουμε ότι ο πλλαπλασιασμός γίνεται $\bmod(x^n - 1)$ *.)*

Απόδειξη. Από το θεώρημα 2.6.16 έχουμε ότι $\mathcal{C} = \langle \gamma(x) \rangle$. Έστω $c(x) \in \mathcal{C}$, τότε υπάρχει $\alpha(x) \in \mathcal{R}_n$ έτσι ώστε $c(x) = \alpha(x) \cdot \gamma(x)$, τότε $c(x) \cdot \delta(x) = \alpha(x) \cdot \gamma(x) \cdot \delta(x) = 0(\bmod(x^n - 1)$.

Αντίστροφα, υποθέτουμε ότι $c(x) \cdot \delta(x) = 0(\bmod(x^n - 1)$. Από την ταυτότητα της διαίρεσης στο $\mathbb{F}[x]$ έχουμε ότι υπάρχουν πολυώνυμα $\pi(x)$, $\upsilon(x) \in \mathbb{F}[x]$ τέτοια ώστε $c(x) = \pi(x) \cdot \gamma(x) + \upsilon(x)$ με $\upsilon(x) = 0$ ή $deg(\upsilon(x)) < deg(\gamma(x)) = n - k$. Τότε από τη σχέση $c(x) \cdot \delta(x) = 0(\bmod(x^n - 1)$ έπεται ότι $\upsilon(x) \cdot \delta(x) = 0(\bmod(x^n - 1)$. Αυτό σημαίνει ότι το πολυώνυμο $x^n - 1$ διαιρεί το $\upsilon(x) \cdot \delta(x)$ στο $\mathbb{F}[x]$. Αλλά ο βαθμός του γινομένου $\upsilon(x) \cdot \delta(x)$ είναι μικρότερος του $(n - k) + k = n$, άτοπο άρα $\upsilon(x) = 0$ και επομένως $c(x) = \pi(x) \cdot \gamma(x) \in \mathcal{C}$.

□

Η ισότητα $c(x) \cdot \delta(x) = 0(\bmod(x^n - 1)$ επάγει κατά ένα φυσιολογικό τρόπο μια σχέση *ορθογωνιότητας* στο $\mathcal{R}_n$, η οποία οδηγεί στον υπολογισμό ένος πίνακα ελέγχου ισοτιμίας για έναν κυκλικό κώδικα, καθώς και στην περιγραφή του δυϊκού του κώδικα.

Θεώρημα 2.6.25. *Έστω $\mathcal{C}$ ένας $[n, k]$ κυκλικός κώδικας με γεννήτορα πολυώνυμο $\gamma(x)$ και πολυώνυμο ελέγχου $\delta(x) = h_0 + h_1 x + \cdots + h_k x^k$. Τότε*

ένας πίνακας ελέγχου ισοτιμίας του κώδικα $\mathcal{C}$ είναι ο ο $(n-k)\times n$ πίνακας $\mathrm{H} = \begin{pmatrix} h_k & h_{k-1} & \cdots & h_0 & 0 & 0 & \cdots & 0 \\ 0 & h_k & \cdots & h_1 & h_0 & 0 & \cdots & 0 \\ \vdots & \vdots & \cdots & \vdots & \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & 0 & h_k & h_{k-1} & \cdots & h_0 \end{pmatrix}$ *επιπλέον ο δυϊκός κώδικας $\mathcal{C}^\perp$ είναι και αυτός κυκλικός και παράγεται από το πολυώνυμο $d(x) = h_k + h_{k-1}x + \cdots + h_0x^k$.*

Απόδειξη. Από το προηγούμενο θεώρημα έχουμε ότι το πολυώνυμο $c(x) = c_0 + c_1x + \cdots + c_{n-1}x^{n-1}$ ανήκει στον κώδικα $\mathcal{C}$ αν και μόνο αν $c(x)\cdot\delta(x) = 0$. Εδώ ο πολλαπλασιασμός είναι $(\mathrm{mod}(x^n-1)$. Αυτό σημαίνει ότι το πολυώνυμο x^n-1 πρέπει να διαιρεί το γινόμενο $c(x)\cdot\delta(x)$. Κάνοντας τον πολλαπλασιασμό $c(x)\cdot\delta(x)$ και απαιτώντας το υπόλοιπο της διαίρεσης με το x^n-1 να είναι ίσον με 0 έχουμε ότι οι συντελεστές των x^k, x^{k+1}, ... , x^{n-1} πρέπει να είναι 0. Δηλαδή έχουμε ότι

$$\begin{array}{ccccccccccc} c_0h_k & + & c_1h_{k-1} & + & \cdots & + & c_kh_0 & = & 0 \\ c_1h_k & + & c_2h_{k-1} & + & \cdots & + & c_{k+1}h_0 & = & 0 \\ \vdots & & \vdots & & \vdots & & \vdots & & \vdots & \vdots & \\ c_{n-k-1}h_k & + & c_{n-k}h_{k-1} & + & \cdots & + & c_{n-1}h_0 & = & 0 \end{array} .$$

Από τις τελευταίες σχέσεις βλέπουμε ότι η (κωδικο)λέξη $c_0\,c_1\cdots c_{n-1}$ είναι ορθογώνια ως πρός τη λέξη $h_k\,h_{k-1}\cdots h_0\,0\cdots 0$ και τις λέξεις που προέρχονται από κυκλικές μεταθέσεις των χαρακτήρων της. Δηλαδή οι γραμμές του πίνακα H είναι στοιχεία του δυϊκού κώδικα $\mathcal{C}^\perp$. Έχουμε επισημάνει ότι το πολυώνυμο ελέγχου $\delta(x) = h_0 + h_1x + \cdots + h_kx^k$ είναι μονικό, δηλαδή $h_k = 1$, αυτό σημαίνει ότι οι $n-k$ το πλήθος γραμμές του πίνακα H είναι γραμμικά ανεξάρτητες, άρα ο πίνακας H είναι γεννήτορας πίνακας του $\mathcal{C}^\perp$, δηλαδή πίνακας ελέγχου ισοτιμίας του κώδικα $\mathcal{C}$.

Παρατηρούμε ότι $d(x) = h_k + h_{k-1}x + \cdots + h_0x^k = x^k\cdot\delta(x^{-1})$, επομένως από τη σχέση $(x^{-1})^n - 1 = \gamma(x^{-1})\cdot\delta(x^{-1})$ έχουμε $((x^{-1})^n-1)\cdot x^k = \gamma(x^{-1})\cdot x^k\cdot\delta(x^{-1}) = \gamma(x^{-1})\cdot d(x)$, δηλαδή $((x^{-1})^n-1)\cdot x^k\cdot x^{n-k} = x^{n-k}\cdot\gamma(x^{-1})\cdot d(x)$. Από την τελευταία σχέση έπεται ότι $x^n - 1 = (-x^{n-k}\cdot\gamma(x^{-1}))\cdot d(x)$. Επειδή το πολυώνυμο γεννήτορας $\gamma(x)$ είναι βαθμού $n-k$, η έκφραση $-x^{n-k}\cdot\gamma(x^{-1})$ είναι ένα πολυώνυμο με συντελεστές από το σώμα $\mathbb{F}$. Άρα το πολυώνυμο $d(x)$ διαιρεί το x^n-1. Επομένως από την Πρόταση 2.6.20 έχουμε ότι το ιδεώδες $\langle d(x)\rangle$ είναι ένας κυκλικός κώδικας με γεννήτορα πίνακα τον πίνακα H, δηλαδή ο δυϊκός κώδικας $\mathcal{C}^\perp$ είναι κυκλικός.

□

Παρατηρήσεις 2.6.26. 1. Το πολυώνυμο $d(x) = h_k + h_{k-1}x + \cdots + h_0x^k$ παράγει μεν τον δυϊκό κώδικα $\mathcal{C}^\perp$, αλλά δεν είναι το πολυώνυμο γεννήτορας,

διότι δεν είναι μονικό. Το πολυώνυμο γεννήτορας είναι το $h_0^{-1} \cdot d(x)$.

2. Όπως βλέπουμε το πολυώνυμο ελέγχου $\delta(x) = h_0 + h_1 x + \cdots + h_k x^k$ του κυκλικού κώδικα $\mathcal{C}$ δεν παράγει τον δυϊκό κώδικα $\mathcal{C}^\perp$, αλλά τον παράγει το *αμοιβαίο* πολυώνυμο $d(x) = h_k + h_{k-1}x + \cdots + h_0 x^k$ του οποίου οι συντελεστές είναι οι συντελεστές του $\delta(x)$ με την αντίστροφη σειρά.

3. Γενικά το αμοιβαίο πολυώνυμο $\overline{\phi(x)}$ ενός πολυωνύμου $\phi(x) = a_k + a_{k-1}x + \cdots + a_0 x^k$ είναι το πολυώνυμο $x^k \phi(x^{-1})$. Επομένως στη συγκεκριμένη περίπτωση το πολυώνυμο $\delta(x^{-1}) = x^{n-k} d(x)$ ανήκει στον κώδικα $\mathcal{C}^\perp$.

   Επίσης είναι εύκολο να δούμε ότι το αμοιβαίο πολυώνυμο ενός γινομένου πολυωνύμων ισούται με το γινόμενο των αντιστοίχων αμοιβαίων πολυωνύμων των παραγόντων.

4. Από την απόδειξη του προηγουμένου θεωρήματος μπορούμε εύκολα να συνάγουμε το ακόλουθο αποτέλεσμα. Ένας $[n, k, d]$ κυκλικός κώδικας με γενήτορα πολυώνυμο $\gamma(x)$ είναι αυτοδυϊκός αν και μόνο αν $\gamma(x) = -\frac{x^n - 1}{x^{n-k} \cdot \gamma(x^{-1})}$ (γιατί;)

Παράδειγμα 2.6.27. Όπως στο Παράδειγμα 2.6.22, έστω το πολυώνυμο $x^4 - 1 = (x-1)(x+1)(x^2+1) \in \mathbb{Z}_3[x]$. Προφανώς ο κυκλικός κώδικας $\mathcal{C}$ με γεννήτορα πολυώνυμο x^2+1 έχει ως γεννήτορα πίνακα τον πίνακα $\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}$, ως πολυώνυμο ελέγχου το πολυώνυμο $(x-1)(x+1) = x^2 - 1$ και επομένως ως πίνακα ελέγχου ισοτιμίας τον πίνακα $\begin{pmatrix} 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{pmatrix}$.

Έχουμε παρατηρήσει (Παράδειγμα $2.6.12_5$) ότι ο Ο $p-$αδικός κώδικας $\mathcal{E}_n$ που αποτελείται από όλες τις λέξεις μήκους n με άθροισμα χαρακτήρων ίσον με μηδέν είναι ένας κυκλικός κώδικας. Αυτό δεν σημαίνει ότι κάθε γραμμικός κώδικας μηδενικού αθροίσματος είναι κυκλικός.
Για παράδειγμα, ο δυαδικός κώδικας $\{\, 0000,\ 1100,\ 0011,\ 1111 \,\}$ είναι γραμμικός και μηδενικού αθροίσματος, αλλά δεν είναι κυκλικός.
Στο επόμενο θεώρημα δίνουμε έναν χαρακτηρισμό των κυκλικών κωδίκων μηδενικού αθροίσματος.

Θεώρημα 2.6.28. *Έστω ο κυκλικός κώδικας $\mathcal{E}_n$ επί του αλφαβήτου $\mathbb{F}$, του οποίου τα στοιχεία είναι όλες οι λέξεις μήκους n με μηδενικό άθροισμα χαρακτήρων. Το πολυώνυμο γεννήτορας του $\mathcal{E}_n$ είναι το $x-1$ και κάθε κυκλικός κώδικας $\mathcal{C}$ μήκους n με γεννήτορα πολυώνυμο $\gamma(x)$ είναι κώδικας μηδενικού αθροίσματος αν και μόνο αν το $x-1$ διαιρεί το $\gamma(x)$.*

Απόδειξη. Έστω $\mathcal{D}$ ο κυκλικός κώδικας του οποίου το πολυώνυμο γεννήτορας είναι το πολυώνυμο $x-1$. Ο $\mathcal{D}$ είναι διάστασης $n-1$ (Πρόταση 2.6.20) και μηδενικού αθροίσματος, διότι κάθε στοιχείο του είναι της μορφής $-a_1\,(a_1-a_2)\,(a_2-a_3)\cdots(a_{(n-k-1)}-a_{n-k})\,a_{n-k}$ (γιατί;). Επομένως $\mathcal{D}\subseteq\mathcal{E}_n$. Ο κώδικας $\mathcal{E}_n$ δεν είναι διάστασης n, αφού υπάρχουν λέξεις με άθροισμα χαρακτήρων που δεν είναι ίσο με μηδέν. Άρα από τη σχέση $\mathcal{D}\subseteq\mathcal{E}_n$ έχουμε ότι $\mathcal{D}=\mathcal{E}_n$.

Τα υπόλοιπα έπονται από την Πρόταση 2.6.23.

□

Παράδειγμα 2.6.29. Στο Παράδειγμα 2.6.27 ο κυκλικός κώδικας $\mathcal{C}$ με γεννήτορα πολυώνυμο x^2+1 περιέχει λέξεις μη μηδενικού αθροίσματος. Το πολυώνυμο ελέγχου είναι το $(x-1)(x+1)=x^2-1$ και επομένως ο δυϊκός κώδικας $\mathcal{C}^\perp$ είναι κώδικας μηδενικού αθροίσματος.

Έχουμε δει προηγουμένως ότι ένας κυκλικός κώδικας, εκτός από το γεννήτορα πολυώνυμο, ενδέχεται να παράγεται και από άλλο πολυώνυμο. Θα δούμε τώρα ότι για κάθε κυκλικό κώδικα $\mathcal{C}$ μήκους n υπάρχει μοναδικό πολυώνυμο $\epsilon(x)\in\mathcal{R}_n$ με τις ιδιότητες:

α) Το $\epsilon(x)$ παράγει τον κώδικα $\mathcal{C}$.

β) Το $\epsilon(x)$ είναι μοναδιαίο στοιχείο του κώδικα $\mathcal{C}$.

γ) Το $\epsilon(x)$ είναι *αδύναμο*, δηλαδή $(\epsilon(x))^2=\epsilon(x)$.

Έστω $\gamma(x)$ και $\delta(x)$ αντίστοιχα τα πολυώνυμα γεννήτορας και ελέγχου για τον κυκλικό κώδικα $\mathcal{C}$. Από τον τρόπο ορισμού τους $(\gamma(x)\cdot\delta(x)=x^n-1)$ έχουμε ότι είναι σχετικά πρώτα, επομένως υπάρχουν πολυώνυμα $\alpha(x)$, $\beta(x)$ έτσι ώστε

$$\alpha(x)\cdot\gamma(x)+\beta(x)\cdot\delta(x)=1 \qquad (*)\,.$$

Έστω $\epsilon(x)=\alpha(x)\cdot\gamma(x)$. Αν θεωρήσουμε τον πολλαπλασιασμό $\bmod(x^n-1)$ (βλέπε τη σχετική συζήτηση πριν από την Πρόταση 2.6.13 στη σελίδα 110), τότε το πολυώνυμο $\epsilon(x)=\alpha(x)\cdot\gamma(x)$ ανήκει στον κυκλικό κώδικα $\mathcal{C}$. Γνωρίζουμε (Θεώρημα 2.6.24) ότι ένα πολυώνυμο $c(x)\in\mathcal{R}_n$ είναι στοιχείο του κώδικα αν και μόνο αν $c(x)\cdot\delta(x)=0$ (υπενθυμίζουμε ότι ο πολλαπλασιασμός γίνεται $\bmod(x^n-1)$). Επομένως από την σχέση $(*)$ έχουμε ότι $\alpha(x)\cdot\gamma(x)\cdot c(x)+\beta(x)\cdot\delta(x)\cdot c(x)=c(x)$, δηλαδή $\epsilon(x)\cdot c(x)=c(x)$. Η τελευταία σχέση αποδεικνύει ότι το $\epsilon(x)$ είναι αφ' ενός μεν μοναδιαίο στοιχείο του $\mathcal{C}$, αφ' ετέρου παράγει τον $\mathcal{C}$, αφού κάθε στοιχείο του είναι πολλαπλάσιο του $\epsilon(x)$.

Πολλαπλασιάζοντας και τα δύο μέλη της $(*)$ με το $\epsilon(x)$ εύκολα βλέπουμε ότι πράγματι ισχύει $(\epsilon(x))^2=\epsilon(x)$.

Τέλος το $\epsilon(x)$ είναι μοναδικό, διότι γενικά σε έναν δακτύλιο αν υπάρχει μοναδιαίο αυτό είναι μοναδικό.

Παράδειγμα 2.6.30. Έστω το πολυώνυμο $x^4-1 \in \mathbb{Z}_3[x]$. Προφανώς $x^4-1 = (x-1)(x+1)(x^2+1)$. Αν $\mathcal{C}$ είναι ο κυκλικός κώδικας με γεννήτορα πολυώνυμο x^2+1, τότε το πολυώνυμο $\epsilon(x) = 2x^2+2 \in \mathcal{R}_4$ πληροί τις παραπάνω ιδιότητες (να κάνετε τον έλεγχο!)

Παρατήρηση 2.6.31. Το πολυώνυμο $\epsilon(x)$ που πληροί τις παραπάνω ιδιότητες ονομάζεται **αδύναμος γεννήτορας** για τον κυκλικό κώδικα $\mathcal{C}$ και η σχέση $(*)$ μας δίνει τον τρόπο υπολογισμού του, αν γνωρίζουμε το πολυώνυμο γεννήτορα.

Αντίστροφα, αν γνωρίζουμε τον αδύναμο γεννήτορα $\epsilon(x)$ ενός κυκλικού κώδικα $\mathcal{C}$, τότε για το πολυώνυμο γεννήτορα έχουμε
$\gamma(x) = \text{μ.κ.δ.}\,(\epsilon(x),\ x^n-1)$. (Αποδείξτε το!)

Κυκλικοί κώδικες και ρίζες της μονάδας

Όπως είχαμε επισημάνει στην σελίδα 113 το πρόβλημα του προσδιορισμού όλων των κυκλικών κωδίκων μήκους n είναι ισοδύναμο με τον προσδιορισμό της ανάλυσης του πολυωνύμου x^n-1 σε γινόμενο (αναγώγων) πολυωνύμων. Το πρόβλημα αυτό είναι πολύ δύσκολο στη γενικότητά του. Έχουν επινοηθεί διάφορες μέθοδοι "παραγοντοποίησης " του πολυωνύμου x^n-1. Εδώ δεν θα ασχοληθούμε με την παραγοντοποίηση αυτή. Θα τη θεωρήσουμε δεδομένη και θα δώσουμε μια διαφορετική παρουσίαση των κυκλικών κωδίκων χρησιμοποιώντας τις $n-$οστές ρίζες της μονάδας.

Έστω $\mathbb{F}_p$ ένα πεπερασμένο σώμα με $q = p^\nu$ το πλήθος στοιχεία και $x^n-1 \in \mathbb{F}_p[x]$. Υποθέτουμε ότι $x^n-1 = \prod_{i=1}^{k} m_i(x)$ είναι η ανάλυση του σε γινόμενο μονικών αναγώγων πολυωνύμων επί του $\mathbb{F}_p$. Υποθέτουμε ότι ω είναι μια ρίζα του πολυωνύμου x^n-1, η ω βρίσκεται σε μια επέκταση του σώματος $\mathbb{F}_p$ και μηδενίζει έναν (μόνο) από τους παράγοντες $m_i(x)$. Επομένως για ένα πολυώνυμο $f(x) \in \mathbb{F}_p[x]$ έχουμε $f(\omega) = 0$ αν και μόνο αν υπάρχει $\pi(x) \in \mathbb{F}_p[x]$ έτσι ώστε $f(x) = \pi(x)\cdot m_i(x)$. Μεταβαίνοντας στον δακτύλιο πηλίκο $\mathcal{R}_n = \mathbb{F}_p[x]/\langle x^n-1\rangle$ βλέπουμε ότι το ω είναι ρίζα του πολυωνύμου $f(x)$ αν και μόνο αν το $f(x)$ ανήκει στον κυκλικό κώδικα $\langle m_i(x)\rangle$.

Από την προηγούμενη συζήτηση μπορούμε να συνάγουμε το επόμενο θεώρημα.

Θεώρημα 2.6.32. *Έστω $g(x) = r_1(x)\cdot r_2(x)\cdots r_s(x)$ ένα γινόμενο (μονικών) αναγώγων παραγόντων του x^n-1. Υποθέτουμε ότι $\{\rho_1, \rho_2, \ldots, \rho_\nu\}$ είναι οι ρίζες του $g(x)$. Τότε ο κυκλικός κώδικας ο παραγόμενος από το $g(x)$ είναι ίσος με $\mathcal{C} = \langle g(x)\rangle = \{f(x) \in \mathcal{R}_n \mid f(\rho_1) = 0, f(\rho_2) = 0, \ldots, f(\rho_\nu) = 0\}$. Επιπλέον είναι αρκετό να επιλέξουμε μόνο μία ρίζα ξ_i από κάθε ανάγωγο παράγοντα $r_i(x)$, $i = 1, \ldots, s$ και να ισχύει $\mathcal{C} = \langle g(x)\rangle = \{f(x) \in \mathcal{R}_n \mid f(\xi_1) = 0, f(\xi_2) = 0, \ldots, f(\xi_s) = 0\}$.*

Απόδειξη. Οι ρίζες $\{\rho_1, \rho_2, \ldots, \rho_\nu\}$ του πολυωνύμου $g(x)$ ανήκουν στο σώμα ριζών $\mathbb{E}$ του πολυωνύμου x^n-1, επομένως αν ένα πολυώνυμο $f(x) \in \mathcal{R}_n$ ανήκει στον κυκλικό κώδικα $\mathcal{C} = \langle g(x) \rangle$, προφανώς μηδενίζεται από τα $\rho_1, \rho_2, \ldots, \rho_\nu$, άρα $\mathcal{C} = \langle g(x) \rangle \subseteq \{ f(x) \in \mathcal{R}_n \mid f(\rho_1) = 0, f(\rho_2) = 0, \ldots, f(\rho_\nu) = 0 \}$. Αντίστροφα ένα πολυώνυμο $f(x) \in \mathcal{R}_n$, που μηδενίζεται από τα $\rho_1, \rho_2, \ldots, \rho_\nu$, στο σώμα $\mathbb{E}$ θα έχει την ανάλυση $f(x) = g(x) \cdot \pi(x)$ με $\pi(x) \in \mathbb{F}_p[x]$ (γιατί το $\pi(x) \in \mathbb{F}_p[x]$ και όχι γενικά $\pi(x) \in \mathbb{E}[x]$;). Άρα $\mathcal{C} = \langle g(x) \rangle \supseteq \{ f(x) \in \mathcal{R}_n \mid f(\rho_1) = 0, f(\rho_2) = 0, \ldots, f(\rho_\nu) = 0 \}$.

Από κάθε ανάγωγο παράγοντα $r_i(x)$, $i = 1, \ldots, s$ επιλέγουμε μια ρίζα ξ_i. Αν ο βαθμός του $r_i(x)$ είναι d_i, τότε οι άλλες ρίζες του $r_i(x)$ είναι οι $\xi_i^q, \xi_i^{q^2}, \ldots, \xi_i^{q^{d_i-1}}$.
(Όπου $q = p^\nu$ είναι το πλήθος ων στοιχείων του σώματος $\mathbb{F}_p$). Πράγματι, από τη σχέση $(r_i(\xi_i))^q = r_i(\xi_i^q)$ έχουμε ότι οι $\xi_i, \xi_i^q, \xi_i^{q^2}, \ldots, \xi_i^{q^{d_i-1}}$ είναι οι ρίζες του $r_i(x)$, αφού είναι διακεκριμένες. Επομένως έχουμε ότι $\{ f(x) \in \mathcal{R}_n \mid f(\xi_1) = 0, f(\xi_2) = 0, \ldots, f(\xi_s) = 0 \} \subseteq \{ f(x) \in \mathcal{R}_n \mid f(\rho_1) = 0, f(\rho_2) = 0, \ldots, f(\rho_\nu) = 0 \}$. Αλλά προφανώς ισχύει $\{ f(x) \in \mathcal{R}_n \mid f(\xi_1) = 0, f(\xi_2) = 0, \ldots, f(\xi_s) = 0 \} \supseteq \{ f(x) \in \mathcal{R}_n \mid f(\rho_1) = 0, f(\rho_2) = 0, \ldots, f(\rho_\nu) = 0 \}$. Οπότε έπεται το αποτέλεσμα.

□

Παρατηρήσεις 2.6.33. 1. Οι ρίζες $\xi_i, \xi_i^q, \xi_i^{q^2}, \ldots, \xi_i^{q^{d_i-1}}$ του πολυωνύμου $r_i(x)$ είναι πράγματι διακεκριμένες, διότι αν υποθέσουμε ότι $\xi_i^{q^\kappa} = \xi_i^{q^\lambda}$ με $0 \leq \kappa < \lambda \leq d_i - 1$, τότε $\xi_i^{q^\kappa} = \xi_i^{q^\lambda} = (\xi_i^{q^\kappa})^{q^{\lambda-\kappa}}$, δηλαδή $(\xi_i^{q^\kappa})^{q^{\lambda-\kappa}} - \xi_i^{q^\kappa} = 0$. Από την τελευταία σχέση έχουμε ότι το $\xi_i^{q^\kappa}$ είναι ρίζα του πολυωνύμου $x^{q^{\lambda-\kappa}} - x$. Άρα το $\xi_i^{q^\kappa}$ είναι κοινή ρίζα του ανάγωγου πολυωνύμου $r_i(x)$ και του πολυωνύμου $x^{q^{\lambda-\kappa}} - x$. Δηλαδή το $r_i(x)$ διαιρεί το $x^{q^{\lambda-\kappa}} - x$. Από γνωστό Θεώρημα [6] έχουμε ότι ο βαθμός d_i του $r_i(x)$ πρέπει να διαιρεί τη διαφορά $\lambda - \kappa$, άτοπο. Επομένως οι ρίζες $\xi_i, \xi_i^q, \xi_i^{q^2}, \ldots, \xi_i^{q^{d_i-1}}$ είναι διακεκριμένες.

2. Θα μπορούσαμε να αναδιατυπώσουμε το προηγούμενο θεώρημα ως εξής:

   Έστω $\{\rho_1, \rho_2, \ldots, \rho_\nu\}$ κάποιες ρίζες του πολυωνύμου $x^n - 1$, τότε το σύνολο $\{ f(x) \in \mathcal{R}_n \mid f(\rho_1) = 0, f(\rho_2) = 0, \ldots, f(\rho_\nu) = 0 \}$ είναι ένας κυκλικός κώδικας με γεννήτορα πολυώνυμο το ελάχιστο κοινό πολλαπλάσιο των ελαχίστων πολυωνύμων των ριζών $\rho_1, \rho_2, \ldots, \rho_\nu$.

[6] Το Θεώρημα που επικαλούμαστε είναι το εξής:
(Πόρισμα Α'.3.11) Έστω $\mathbb{F}$ πεπερασμένο σώμα με q το πλήθος στοιχεία και $r(x) \in \mathbb{F}[x]$ ανάγωγο πολυώνυμο. Τότε το $r(x)$ διαιρεί το πολυώνυμο $x^{q^n} - x$ αν και μόνο αν ο βαθμός του $r(x)$ διαιρεί το n.

Η απόδειξη είναι προφανής και αφίνεται ως άσκηση.
(Μπορούμε να παραβάλουμε το αποτέλεσμα αυτό με την Πρόταση 2.6.23(2)).

Η θεώρηση αυτή των κυκλικών κωδίκων μας επιτρέπει να υπολογίσουμε έναν πίνακα ελέγχου ισοτιμίας ένος κυκλικού κώδικα με διαφορετικό τρόπο από αυτόν που αναφέρεται στο Θεώρημα 2.6.25.

Έστω $\{\rho_1, \rho_2, \ldots, \rho_\nu\}$ ένα σύνολο ριζών του πολυωνύμου $x^n - 1$. Ένα πολυώνυμο $f(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} \in \mathcal{R}_n$ έχει ρίζα το ρ_i αν και μόνο αν $a_0 + a_1\rho_i + \cdots + a_{n-1}\rho_i^{n-1} = 0$.

Οι ρίζες ρ_i βρίσκονται σε μια επέκταση, έστω $\mathbb{E}$, του σώματος $\mathbb{F}_p$. Το σώμα $\mathbb{E}$ μπορεί να θεωρηθεί ως διανυσματικός χώρος επί του $\mathbb{F}_p$ με διάσταση έστω d. Επιλέγουμε μια βάση του $\mathbb{E}$ ως προς $\mathbb{F}_p$. Για κάθε $i = 1, \ldots, \nu$ και κάθε $j = 0, \ldots, n-1$ θα συμβολίζουμε με $[r_i^j]$ το διάνυσμα στήλη των συντελεστών στην έκφραση του ρ_i^j ως γραμμικού συνδυασμού των στοιχείων αυτής της βάσης με συντελεστές από το σώμα $\mathbb{F}_p$.

Από τη σχέση $a_0 + a_1\rho_i + \cdots + a_{n-1}\rho_i^{n-1} = 0$ έχουμε ότι $a_0 + a_1[r_i] + \cdots + a_{n-1}[r_i^{n-1}] = \mathbf{0}$, όπου $\mathbf{0}$ παριστά το μηδενικό διάνυσμα στήλη.

Η τελευταία σχέση θα μπορούσε να εκφραστεί με τη βοήθεια πινάκων ως εξής:

Κατασκευάζουμε τον πίνακα $\mathrm{P} = \begin{pmatrix} [r_1^0] & [r_1^1] & \cdots & [r_1^{n-1}] \\ [r_2^0] & [r_2^1] & \cdots & [r_2^{n-1}] \\ \vdots & \vdots & \vdots & \vdots \\ [r_\nu^0] & [r_\nu^1] & \cdots & [r_\nu^{n-1}] \end{pmatrix}$.

Ο πίνακας P είναι ένας $\nu \times n$, του οποίου τα στοιχεία (προς το παρόν) είναι διανύσματα στήλες. Οπότε αν θέσουμε ως $\mathbf{a} = (a_0, a_1, \ldots, a_{n-1})$, τότε η σχέση $a_0 + a_1[r_i] + \cdots + a_{n-1}[r_i^{n-1}] = \mathbf{0}$ ισχύει για κάθε $i = 1, \ldots, \nu$ αν και μόνο αν $\mathbf{a} \cdot \mathrm{P}^\perp = \mathbf{0}$.

Στον πίνακα P, αν αναπτύξουμε την κάθε στήλη $[r_i^j]$, η οποία έχει μήκος ίσον με d, τότε ο πίνακας μπορεί να θεωρηθεί ως ένας $\nu d \times n$ πίνακας με στοιχεία από το σώμα $\mathbb{F}_p$. Οπότε από τα προηγούμενα έχουμε ότι είναι ο πίνακας ελέγχου ισοτιμίας για τον κυκλικό κώδικα $\{ f(x) \in \mathcal{R}_n \mid f(\rho_1) = 0, f(\rho_2) = 0, \ldots, f(\rho_\nu) = 0 \}$.

Παρατήρηση 2.6.34. Οι γραμμές του πίνακα που κατασκευάσαμε με τον παραπάνω τρόπο δεν είναι κατ' ανάγκη γραμμικά ανεξάρτητες, οπότε αν θέλουμε να έχουμε έναν γεννήτορα πίνακα του δυϊκού κώδικα πρέπει να διαγράψουμε μερικές από αυτές και να κρατήσουμε το μεγαλύτερο δυνατόν πλήθος γραμμικά ανεξαρτήτων γραμμών.

2.6.3 Ασκήσεις

1. Να υπολογίσετε έναν πίνακα ελέγχου ισοτιμίας και την ελάχιστη απόσταση στις ακόλουθες περιπτώσεις πολυωνυμικών δυαδικών κωδίκων με αντίστοιχα πολυώνυμα γεννήτορες $1+x+x^2$, $1+x+x^3$, $1+x^2, 1+x^3$ και με μήκος 5 ή 8.

2. Στην προηγούμενη άσκηση, σε κάθε περίπτωση, να εξετάσετε ποίοι από τους αντίστοιχους δυϊκούς κώδικες είναι πολυωνυμικοί.

3. Να δώσετε ικανή και αναγκαία συνθήκη ώστε ένας πολυωνυμικός κώδικας να είναι κώδικας μέγιστης απόστασης.

4. Ποίοι από τους ακόλουθους κώδικες είναι κυκλικοί; Στην περίπτωση που κάποιος είναι κυκλικός υπολογίστε το πολυώνυμο γεννήτορα και τον πίνακα ελέγχου ισοτιμίας.

   i) $\mathcal{C} = \{\, 00000,\, 10110,\, 01101,\, 11011 \,\}$.

   ii) $\mathcal{D} = \{\, \mathbf{x} \in \mathbb{Z}_3^n \mid w(\mathbf{x}) \equiv 0, \mathrm{mod} 3 \,\}$.

   iii) $\mathcal{E} = \{\, x_1x_2\cdots x_n \in \mathbb{Z}_3^n \mid \sum_{i=1}^n \equiv 0 \,\mathrm{mod} 3 \,\}$.

5. Έστω $\mathcal{C}$ ο δυαδικός κυκλικός κώδικας μήκους 7 με γενήτορα πολυώνυμο x^3+x+1. Να υπολογίσετε έναν πίνακα ελέγχου ισοτιμίας του $\mathcal{C}$. Στον πίνακα που θα βρείτε να εφαρμόσετε μια μετάθεση στις στήλες του έτσι ώστε ο γραμμικός κώδικας που έχει ως πίνακα ελέγχου ισοτιμίας τον νέο πίνακα να μην είναι κυκλικός. Άρα να συμπεράνετε ότι υπάρχουν κυκλικοί κώδικες που είναι ισοδύναμοι με μη κυκλικούς κώδικες.

6. Έστω $\mathcal{C}$ ένας γραμμικός κώδικας με γεννήτορα πίνακα G. Δείξτε ότι αρκεί από κάθε κυκλική μετάθεση των στοιχείων κάθε γραμμής του πίνακα G να προκύπτει μια (κωδικο)λέξη για να είναι ο κώδικας κυκλικός.

7. Δείξτε ότι ο δυαδικός κυκλικός κώδικας $\mathcal{C}$ με γεννήτορα πολυώνυμο $\gamma(x)$ περιέχει την λέξη $11\cdots 1$ αν και μόνο αν $\gamma(1) \neq 0$.

8. Έστω $\mathcal{C}$ ένας κυκλικός δυαδικός κώδικας περιττού μήκους. Δείξτε ότι ο $\mathcal{C}$ περιέχει μια (κωδικο)λέξη περιττού βάρους αν και μόνο αν $11\cdots 1 \in \mathcal{C}$.

9. Έστω $\mathcal{C}$ ένας κυκλικός δυαδικός κώδικας με γεννήτορα πολυώνυμο $\gamma(x)$. Υποθέτουμε ότι ο $\mathcal{C}$ περιέχει τουλάχιστον μια (κωδικο)λέξη περιττού βάρους. Δείξτε ότι το υποσύνολο όλων των (κωδικο)λέξεων αρτίου βάρους αποτελεί έναν κυκλικό υποκώδικα και να υπολογίσετε το πολυώνυμο γεννήτορα.

10. Έστω p ένας πρώτος αριθμός και n ένας θετικός ακέραιος. Υπάρχει $p-$αδικός κυκλικός κώδικας μήκους n; (να διακρίνετε πρώτα την περίπτωση αν οι p και n είναι σχετικά πρώτοι).

11. Πόσοι τριαδικοί κυκλικοί κώδικες μήκους 8 υπάρχουν; Για καθέναν από αυτούς να βρείτε έναν πίνακα ελέγχου ισοτιμίας.

12. Να βρεθούν όλοι οι δυαδικοί κυκλικοί κώδικες μήκους 7. Για κάθε έναν από αυτούς να βρείτε το πολυώνυμο ελέγχου και έναν αδύναμο γεννήτορα. Ποίοι απ' αυτούς είναι ελάχιστοι, ποίοι μέγιστοι; Να κάνετε ένα διάγραμμα όπου να διατάξετε όλους αυτούς τους κώδικες ως προς τη σχέση "του περιέχεσθαι". (Θεωρήστε γνωστό ότι $x^7-1=(x-1)(x^3+x+1)(x^3+x^2+1)$).

13. Έστω $\mathcal{C}$ ένας κυκλικός κώδικας με γεννήτορα πολυώνυμο $\gamma(x)$. Υποθέτουμε ότι ο $\mathcal{C}$ είναι αυτο-ορθογώνιος (δηλαδή $\mathcal{C}\subseteq\mathcal{C}^{\perp}$). Δείξτε ότι το $x-1$ διαιρεί το $\gamma(x)$.

14. Δείξτε ότι ο κυκλικός κώδικας $\mathcal{C}$ με γεννήτορα πολυώνυμο $\gamma(x)$ και πολυώνυμο ελέγχου $\delta(x)$ είναι αυτο-ορθωγώνιος αν και μόνο αν το αμοιβαίο πολυώνυμο του $\delta(x)$ διαιρεί το $\gamma(x)$.

15. Έστω $\mathcal{C}$ ένας κυκλικός μήκους n κώδικας με γεννήτορα πολυώνυμο $\gamma(x)$. Υποθέτουμε ότι ο δυϊκός κώδικας $\mathcal{C}^{\perp}$ έχει γεννήτορα πολυώνυμο το πολυώνυμο $d(x)$. Αν $x^n-1=\gamma(x)\cdot\sigma(x)$, δείξτε ότι για κάθε ρίζα ξ του πολυωνύμου $d(x)$ το ξ^{-1} είναι ρίζα του $\sigma(x)$.

16. Ένας κώδικας λέγεται **αναστρέψιμος** αν για κάθε (κωδικο)λέξη $\mathbf{c}=c_0c_1\cdots c_{n-1}$ έπεται ότι και η λέξη $c_{0\nu-1}c_{n-2}\cdots c_0$ είναι στοιχείο του κώδικα. Δείξτε ότι ο κυκλικός κώδικας $\mathcal{C}$ ένας κυκλικός κώδικας με γεννήτορα πολυώνυμο $\gamma(x)$ είναι αναστρέψιμος αν και μόνο αν για κάθε ρίζα ξ του πολυωνύμου $\gamma(x)$ έπεται ότι και η ξ^{-1} είναι ρίζα του $\gamma(x)$.

17. Να δώσετε ικανή και αναγκαία συνθήκη ώστε ένας κυκλικός κώδικας να είναι κώδικας μέγιστης απόστασης.

Κεφάλαιο 3

"Καλοί" Κώδικες

Πολλές φορές προηγουμένως αναφερθήκαμε στις ιδιότητες που έχει ένας κώδικας, π.χ. ως προς την αποτελεσματικότητά του να ανιχνεύει ή (και) διορθώνει λάθη, ως προς το πλήθος των πληροφοριών που μπορεί να μεταδοθούν μέσω του κώδικα, ως προς την ευκολία που πραγματοποιείται η κωδικοποίηση και η αποκωδικοποίηση κ.λ.π. Τα κριτήρια επιλογής ενός κώδικα ποικίλουν από περίπτωση σε περίπτωση και εξαρτώνται τόσο από τη φύση του προς κωδικοποίηση μηνύματος, όσο και από τα διαθέσιμα μέσα για αποθήκευση/αποστολή του μηνύματος. Επιπλέον ο χαρακτηριμός ενός κώδικα ως "καλού" εμπεριέχει και υποκειμενικά κριτήρια και μάλλον θα ήταν προτιμότερο να αναφέρονται ως "βολικοί" κώδικες.

Στις επόμενες παραγράφους θα αναφερθούμε σε ορισμένες κατηγορίες κωδίκων οι οποίοι είναι γραμμικοί. Ο τρόπος που ορίζονται είναι τέτοιος ώστε να μας εξαφαλίζει ένα αποτελεσματικό τρόπο χειρισμού των. Από ιστορικής πλευράς είναι κώδικες οι οποίοι έχουν επινοηθεί και χρησιμοποιηθεί με επιτυχία σε πολλές περιπτώσεις. Μάλιστα οι περισσότεροι εξακολουθούν να χρησιμιποιούνται μέχρι σήμερα.

3.1 Κώδικες Hamming

Οι κώδικες Hamming είναι από τους πλέον γνωστούς κώδικες που χρησιμοποιούνται. Το πλεονέκτημά τους (αν και δεν μπορούν να διορθώσουν μεγάλο αριθμό λαθών) έγκειται στο γεγονός ότι η αποκωδικοποίηση είναι εύκολη και επιτυνχάνεται με ιδιαίτερα κομψό τρόπο.

Επινοήθηκαν, ανεξάρτητα, από τους Marcel Golay το 1949 και Richard Hamming το 1950 και λόγω της πλεονεκτημάτων τους εξακολουθούν και σήμερα

να είναι σε χρήση.

Συμφωνα με την Πρόταση 2.2.27 η ελάχιστη απόσταση ενός $[n,\, k]$ γραμμικού κώδικα με πίνακα ελέγχου ισοτιμίας Η είναι ο μικρότερος θετικός ακέραιος d για τον οποίο υπάρχουν d το πλήθος γραμμικά εξαρτημένες στήλες στον πίνακα Η. Η πιο απλή ενδιαφέρουσα περίπτωση είναι να μην υπάρχουν δύο γραμμικά εξατρημένες στήλες, δηλαδή καμία στήλη να μην είναι πολλαπλάσιο κάποιας άλλης. Επομένως, εάν θέλουμε να κατασκευάσουμε έναν $[n,\, k,\, 3]$ γραμμικό κώδικα, πρέπει και αρκεί να κατασκευάσουμε έναν $(n-k)\times n$ πίνακα του οποίου ανα δύο οι στήλες να είναι γραμμικά ανεξάρτητες, αλλά να υπάρχει (τουλάχιστον) ένα σύνολο τριών γραμμικά εξαρτημένων στηλών. Ο πίνακας αυτός θα είναι ο πίνακας ελέγχου ισοτιμίας του κώδικα.

Η διαδικασία κατασκευής ενός τέτοιου πίνακα είναι απλή, μάλιστα δε μπορούμε να κατασκευάσουμε τέτοιους πίνακες με το μεγαλύτερο δυνατό πλήθος στηλών.

Έστω r ένας θετικός ακέραιος, $\mathbb{F}_p$ ένα πεπερασμένο σώμα με $q = p^m$ το πλήθος στοιχεία, το οποίο θα είναι το αλφάβητο και $V_1 = \mathbb{F}_p^r$. Επιλέγουμε ένα μη μηδενικό διάνυσμα $\mathbf{c_1} \in V_1$ και θέτουμε $V_2 = V_1 \setminus \{\, \lambda \mathbf{c_1} \mid \lambda \in \mathbb{F}_p,\, \lambda \neq 0 \,\}$. Τώρα επιλέγουμε ένα μη μηδενικό διάνυσμα $\mathbf{c_2} \in V_2$ και θέτουμε $V_3 = V_2 \setminus \{\, \lambda \mathbf{c_2} \mid \lambda \in \mathbb{F}_p,\, \lambda \neq 0 \,\}$. Η διαδικασία αυτή συνεχίζεται έως ότου εξαντληθούν όλα τα μη μηδενικά στοιχεία του $\mathbb{F}_p^r$. Ας υπολογίσουμε όλα τα στοιχεία του $\mathbb{F}_p^r$ που μπορούν να επιλεγούν με αυτή τη διαδικασία. Τα μη μηδενικά στοιχεία του σώματος είναι $q-1$, επομένως σε κάθε βήμα εξαιρούμε $|\, \{\, \lambda \mathbf{c_2} \mid \lambda \in \mathbb{F}_p,\, \lambda \neq 0 \,\} \,| = q-1$ στοιχεία, Το σύνολο $\mathbb{F}_p^r$ έχει $q^r - 1$ στοιχεία. Επομένως τελικά μπορούμε να επιλέξουμε $(q^r-1)/(q-1)$ το πλήθος στοιχεία με αυτή τη διαδικασία.

Με άλλα λόγια διαμερίζουμε το σύνολο $\mathbb{F}_p^r$ σε κλάσεις, όπου κάθε κλάση περιέχει όλα τα μη μηδενικά πολλαπλάσια ενός μη μηδενικού διανύσματος (υπάρχουν $(q^r-1)/(q-1)$ το πλήθος τέτοιες κλάσεις) και από κάθε κλάση επιλέγουμε ένα διάνυσμα.

Με τα διανύσματα που επιλέξαμε κατασκευάζουμε έναν $r\times n$ πίνακα Η, όπου $n = (q^r-1)/(q-1)$.

Από το Πόρισμα 2.2.14 έπεται ότι υπάρχει μοναδικός γραμμικός κώδικας με πίνακα ελέγχου ισοτιμίας τον πίνακα Η, ο οποίος, από τον τρόπο κατασκευής του, έχει ελάχιστη απόσταση ίση με 3 και διάσταση ίση με $k = ((q^r-1)/(q-1)) - r$.

Ορισμός 3.1.1. *Ο γραμμικός κώδικας* $[n = (q^r-1)/(q-1),\, k = ((q^r-1)/(q-1)) - r,\, 3]$ *που κατασκευάσαμε με την παραπάνω διαδικασία ονομάζεται* $q-$*αδικός* **Hamming** *κώδικας και συμβολίζεται* $\mathcal{H}(r,\, q)$. *Ο πίνακας ελέγχου ισοτιμίας* Η *ονομάζεται πίνακας* **Hamming** .

Παραδείγματα 3.1.2. 1. Ένας πίνακας ελέγχου ισοτιμίας για τον κώδικα

$\mathcal{H}(2,\,2)$ είναι ο $\mathrm{H} = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}$. Οπότε ο γεννήτορας πίνακας είναι ο $\mathrm{G} = \begin{pmatrix} 1 & 1 & 1 \end{pmatrix}$. Δηλαδή ο κώδικας $\mathcal{H}(2,\,2)$ είναι ο επαναληπτικός κώδικας $\{000,\,111\}$.

2. Ένας πίνακας ελέγχου ισοτιμίας για τον κώδικα $\mathcal{H}(3,\,2)$ είναι ο $\mathrm{H} = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$.

3. Ένας πίνακας ελέγχου ισοτιμίας για τον κώδικα $\mathcal{H}(2,\,11)$ είναι ο $\mathrm{H} = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \end{pmatrix}$.

   Ο κώδικας που μελετήσαμε στο Παράδειγμα 2.2.28 προέρχεται από διπλή σύμπτυξη του κώδικα $\mathcal{H}(2,\,11)$, αφού ο πίνακας ελέγχου ισοτιμίας του προέρχεται από τον παραπάνω πίνακα H διαγράφοντας τις δύο πρώτες στήλες.

4. Ένας πίνακας ελέγχου ισοτιμίας για τον κώδικα $\mathcal{H}(3,\,3)$ είναι ο $\mathrm{H} = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 \\ 1 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 \end{pmatrix}$.

Θεώρημα 3.1.3. *Ένας $\mathcal{H}(r,\,q)$ κώδικας είναι τέλειος και διορθώνει μόνο ένα λάθος.*

Απόδειξη. Η απόδειξη είναι άμεση συνέπεια της Πρότασης 1.5.12 και για το λόγο αυτό αφίνεται ως άσκηση.

□

Παρατηρήσεις 3.1.4. 1. Από τον τρόπο κατασκευής ενός κώδικα Hamming έχουμε πολλές δυνατότητες για την επιλογή των διανυσμάτων που θα αποτελέσουν τις στήλες του πίνακα ελέγχου ισοτιμίας, επομένως μπορούμε να κατασκευάσουμε πολλούς $\mathcal{H}(r,\,q)$ κώδικες, οι οποίοι όμως είναι ισοδύναμοι. Όπως έχουμε επισημάνει ισοδύναμοι κώδικες ταυτίζονται, για το λόγο αυτό στα επόμενα θα λέμε ο $\mathcal{H}(r,\,q)$ κώδικας.

   Ένας εύκολος τρόπος κατασκευής ενός πίνακα ελέγχου ισοτιμίας για έναν $\mathcal{H}(r,\,q)$ κώδικα είναι ο ακόλουθος.

   Ως στήλες λαμβάνουμε κατά (αύξουσα) σειρά όλους τους αριθμούς που έχουν r το πλήθος ψηφία, όταν γραφούν σε $q-$αδική μορφή, των οποίων το πρώτο μη μηδενικό ψηφίο είναι ίσο με 1 (μεταξύ των πολλαπλασίων ενός μη μηδενικού διανύσματος υπάρχει μόνο ένα, του οποίου η η πρώτη μη μηδενική

συντεταγμένη ισούται με 1). Σε όλα τα προηγούμενα παραδείγματα, εκτός του πρώτου οι πίνακες ελέγχου ισοτιμίας έχουν κατασκευασθεί με αυτόν τον τρόπο.

2. Κατασκευάζοντας έναν πίνακα ελέγχου ισοτιμίας σύμφωνα με τον προηγούμενο τρόπο, υπάρχουν r το πλήθος διαφορετικές στήλες των οποίων τα στοιχεία είναι όλα 0 εκτός ενός το οποίο είναι το 1 (γιατί;). Επομένως μπορούμε να πάρουμε έναν ισοδύναμο κώδικα με πίνακα ελέγχου ισοτιμίας της μορφής $\mathrm{H} = [B\, I_r]$. Σύμφωνα με το Θεώρημα 2.2.17 ένας γεννήτορας πίνακας του κώδικα είναι ο $\mathrm{G} = [I_{n-r} - B^t]$, όπου $n = (q^r - 1)/(q - 1)$. Στην περίπτωση αυτή έχουμε έναν συστηματικό κώδικα (βλέπε σελίδα 63) με όλα τα πλεονεκτήματα αποκωδικοποίησης.

3. Οι πλέον συνηθισμένοι κώδικες Hamming είναι οι δυαδικοί. Εδώ οι στήλες ενός πίνακα ελέγχου ισοτιμίας είναι οι ακέραιοι από το 1 έως το $2^r - 1$ εκφρασμένοι σε δυαδική μορφή.

4. Από τον τρόπο ορισμού οι κώδικες Hamming είναι γραμμικοί. Υπάρχουν όμως και μη γραμμικοί κώδικες οι οποίοι έχουν τις ίδιες παραμέτρους με έναν κώδικα Hamming.

   Έστω ο κώδικας $\mathcal{H}(r, 2)$ και $\vartheta : \mathcal{H}(r, 2) \longrightarrow \mathbb{Z}_2$ μια μη γραμμική απεικόνιση με $\vartheta(0) = 0$. Επομένως υπάρχουν $\mathbf{c}, \mathbf{d} \in \mathcal{H}(r, 2)$ έτσι ώστε $\vartheta(\mathbf{c} + \mathbf{d}) \neq \vartheta(\mathbf{c}) + \vartheta(\mathbf{d})$. Για $\mathbf{x} \in \mathbb{Z}_2^n$ ορίζουμε $\pi(\mathbf{x}) = 0$ αν το $\mathbf{x}$ έχει άρτιο βάρος και $\pi(\mathbf{x}) = 1$ αν το $\mathbf{x}$ έχει περιττό βάρος.

   Θεωρούμε τον κώδικα $\mathcal{D} = \{\, (\mathbf{x}\,\mathbf{x}+\mathbf{c}\,\pi(\mathbf{x})+\vartheta(\mathbf{c})) \mid \mathbf{x} \in \mathbb{Z}_2^n,\ \mathbf{c} \in \mathcal{H}(r, 2)\,\}$ με $n = 2^r - 1$. Το μήκος του κώδικα $\mathcal{D}$ προφανώς είναι ίσο με $n+n+1 = 2^{r+1} - 1$. Το μέγεθός του είναι ίσο με $2^{2n+1-(r+1)}$ (γιατί;) και η διάστασή του ίση με τρία. Επομένως έχουμε ένα κώδικα με παραμέτρους όπως οι παράμετροι ενός κώδικα Hamming, ο οποίος προφανώς δεν είναι γραμμικός.

5. Από το προηγούμενο Θεώρημα έπεται άμεσα ότι για $n = (q^r - 1)/(q - 1)$ ισχύει ότι $A_q(n, 3) = q^{n-r}$, δηλαδή έχουμε απαντήσει στο πρόβλημα του προσδιορισμού του $A_q(n, 3)$ (βλέπε Παράγραφο 1.5.2) για άπειρες τιμές του n (αλλά της παραπάνω μορφής).

3.1.1 Αποκωδικοποίηση με κώδικες Hamming

Στη δεύτερη από τις προηγούμενες παρατηρήσεις είδαμε ότι ένας κώδικας Hamming είναι ισοδύναμος με έναν συστηματικό κώδικα. Αν όμως έχουμε έναν πίνακα ελέγχου ισοτιμίας στη μορφή που περιγράφεται στην πρώτη παρατήρηση,

τότε η αποκωδικοποίηση γίνεται ευκολότερα επιτυγχάνοντας όχι μόνο τη διόρθωση ενός λάθους αλλά εντοπίζοντας και τη θέση στην οποία επήλθε η αλλοίωση του χαρακτήρα.

Έστω ότι έχουμε τον κώδικα $\mathcal{H}(r, q)$ με πίνακα ελέγχου ισοτιμίας H στη μορφή που περιγράφεται παραπάνω και κατά την μετάδοση υπεισήλθε το διάνυσμα λάθους $(0, 0, \ldots, a, \ldots, 0)$, όπου το a βρίσκεται στην i θέση. Το σύνδρομό του (βλέπε Παράγραφο 2.3.4) είναι ίσο με $(0, 0, \ldots, a, \ldots, 0) \cdot \mathrm{H}^{\perp}$, δηλαδή η i στήλη του πίνακα H πολλαπλασιασμένη με a. Από τον τρόπο κατασκευής του πίνακα το a είναι το πρώτο μη μηδενικό ψηφίο του συνδρόμου. Επιπλέον πολλαπλασιάζοντας το σύνδρομο με a^{-1} μπορούμε να εντοπίσουμε την θέση του λάθους.

Για παράδειγμα ας πάρουμε τον πίνακα ελέγχου ισοτιμίας

$$\mathrm{H} = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 \\ 1 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 \end{pmatrix}$$ για τον κώδικα $\mathcal{H}(3, 3)$.

Υποθέτουμε ότι λάβαμε τη λέξη $\mathbf{x} = 1101112211201$, το σύνδρομό της είναι το $(1101112211201) \cdot \mathrm{H}^{\perp} = (201) = 2(102)$. Η στήλη $(102)^t$ είναι η εβδόμη στήλη του πίνακα H, επομένως αφαιρώντας το λάθος 2 από την εβδόμη θέση της λέξης $\mathbf{x}$ έχουμε την (κωδικο)λέξη $\mathbf{c} = 1101110211201$ που εστάλη.

Στην περίπτωση όπου ο κώδικας είναι δυαδικός, η όλη διαδικασία είναι ευκολότερη καθότι αν ένα λάθος έχει υπεισέλθει στην i θέση, τότε η i στήλη του πίνακα ελέγχου ισοτιμίας είναι το σύνδρομο της λέξης που ελήφθει. Επιπλέον δε η στήλη i δεν είναι τίποτε άλλο παρά ο αριθμός i εκφρασμένος σε δυαδική μορφή. Οπότε κατευθείαν από το σύνδρομο μιας λέξης που λάβαμε έχουμε τη θέση του λάθους που υπεισήλθε.

3.1.2 Ο δυϊκός ενός κώδικα Hamming

Θα εξετάσουμε το δυϊκό κώδικα ενός κώδικα Hamming μόνο στην περίπτωση που ο κώδικας είναι δυαδικός.

Έστω $\mathcal{H}(r, 2)$ ο δυαδικός κώδικας Hamming με παραμέτρους $[2^r - 1, 2^r - 1 - r, 3]$. Ένας πίνακας Hamming H_r αποτελεί τον πίνακα ελέγχου ισοτιμίας του. Επομένως, επειδή οι γραμμές του είναι γραμμικά ανεξάρτητες, αποτελεί ένα γεννήτορα πίνακα του δυϊκού κώδικα $\mathcal{H}(r, 2)^{\perp} =: \mathcal{S}(r)$. Ο κώδικας $\mathcal{S}(r)$ έχει μήκος ίσο με 2^{r-1} και διάσταση ίση με r. Σε αντίθεση με την ελάχιστη απόσταση του $\mathcal{H}(r, 2)$ που είναι ίση με 3, η απόσταση του $\mathcal{S}(r)$ είναι αρκετά μεγάλη και εξαρτάται από το r. Πριν υπολογίσουμε την ελάχιστη απόσταση θα δούμε πώς υπολογίζουμε επαγωγικά τους πίνακες H_r για $r \geq 1$.

Πρόταση 3.1.5. *Ο πίνακας* H_1 *είναι ο* 1×1 *πίνακας 1 και για* $r \geq 1$ *ισχύει*

$$\mathrm{H}_{r+1} = \left(\begin{array}{ccc|c|ccc} 0 & \cdots & 0 & 1 & 1 & \cdots & 1 \\ \hline & & & 0 & & & \\ & \mathrm{H}_r & & \vdots & & \mathrm{H}_r & \\ & & & 0 & & & \end{array}\right).$$

Απόδειξη. Η απόδειξη είναι απλή αρκεί να δούμε τον τρόπο κατασκευής των πινάκων Hamming που αναφέρουμε στην Παρατήρηση $3.1.4_1$.

□

Αυτός ο τρόπος κατασκευής των πινάκων μας επιτρέπει να περιγράψουμε (επαγωγικά) τα στοιχεία του κώδικα $\mathcal{S}(r+1)$ με τη βοήθεια των στοιχείων του $\mathcal{S}(r)$.

Ως γνωστόν $\mathcal{S}(r+1) = \{\, \mathbf{c} \cdot \mathrm{H}_{r+1} \mid \mathbf{r} \in \mathbb{Z}_2^{r+1} \,\}$. Αν δούμε το στοιχείο $\mathbf{r} \in \mathbb{Z}_2^{r+1}$ ως $a\mathbf{s}$ με $a = 0, 1$ και $\mathbf{s} \in \mathbb{Z}_2^r$, τότε από την μορφή του πίνακα H_{r+1} έχουμε ότι $\mathbf{r} \cdot \mathrm{H}_{r+1} = (a\mathbf{s}) \cdot \mathrm{H}_{r+1} = (\mathbf{s} \cdot \mathrm{H}_r)\, a\, (a\mathbf{1} + \mathbf{s} \cdot \mathrm{H}_r)$. Από την τελευταία σχέση βλέπουμε ότι το τυχαίο στοιχείο $\mathbf{c} \in \mathcal{S}(r+1)$ γράφεται στην μορφή $\mathbf{d}a(a\mathbf{1} + \mathbf{d})$ με $\mathbf{d} \in \mathcal{S}(r)$ και $a = 0$ ή 1.

Στην πραγματικότητα έχουμε αποδείξει την επόμενη πρόταση.

Πρόταση 3.1.6. *Για τον κώδικα* $\mathcal{S}(r)$ *ισχύει:*

1. $\mathcal{S}(1) = \mathbb{Z}_2$
2. *Για* $r \geq 1$ $\mathcal{S}(r+1) = \{\, \mathbf{d}0\mathbf{d} \ \mu\epsilon\ \mathbf{d} \in \mathcal{S}(r) \,\} \cup \{\, \mathbf{d}1\mathbf{d}^c \ \mu\epsilon\ \mathbf{d} \in \mathcal{S}(r) \,\}$
3. *Η ελάχιστη απόσταση του* $\mathcal{S}(r)$ *είναι ίση με* 2^{r-1}. *Επιπλέον η απόσταση μεταξύ δύο (οποιωνδήποτε) στοιχείων του* $\mathcal{S}(r)$ *είναι ίση με* 2^{r-1}.

Απόδειξη. Το μεγαλύτερο μέρος της απόδειξης έχει προηγηθεί. Όσον αφορά την απόσταση μεταξύ δύο (κωδικο)λέξεων μπορούμε επαγωγικά να την υπολογίσουμε αν παρατηρήσουμε την μορφή των στοιχείων του κώδικα $\mathcal{S}(r)$. □

Παρατηρήσεις 3.1.7.

1. Επειδή όλες οι (κωδικο)λέξεις του κώδικα $\mathcal{S}(r)$ ισαπέχουν, έχει επικρατήσει οι κώδικες αυτοί να ονομάζονται κώδικες **Simplex** , καθότι μπορούμε να φαντασθούμε ότι τα στοιχεία τους καταλαμβάνουν τις κορυφές ενός (πολυδιάστατου) simplex. Στην περίπτωση όπου $r = 2$ είναι εύκολο να δούμε τα στοιχεία του $\mathcal{S}(2)$ ως τις κορυφές ενός κανονικού τετραέδρου.

2. Η ελάχιστη απόσταση του κώδικα $\mathcal{H}(r, 2)$ είναι ίση με τρία ένω το μέγεθος του είναι πολύ μεγάλο. Επομένως το επιρτεπόμενο μέγεθος της μεταδιδόμενης πληροφορίας είναι μεγάλο σε αντίθεση με το πλήθος των λαθών τα

οποία μπορούν να διορθωθούν.
Από την άλλη πλευρά ο δυϊκός κώδικας $\mathcal{H}(r,\,2)^{\perp} =: \mathcal{S}(r)$ έχει μικρό μέγεθος, άρα περιορισμένη δυνατότητα στη μετάδοση μεγάλου όγκου πληροφοριών, αλλά η ελάχιστη απόστασή του επιτρέπει να διορθώνονται σχεδόν το $25^{\circ}/_{\circ}$ των μεταδιδόμενων χαρακτήρων.

3.1.3 Οι κώδικες Hamming ως κυκλικοί κώδικες

Η παρουσίσαση των κυκλικών κωδίκων με τη βοήθεια των $n-$οστών ριζών της μονάδας (βλέπε σελίδα 120) μας επιτρέπει να δούμε ότι μερικοί από τους κώδικες Hamming είναι ισοδύναμοι με κυκλικούς κώδικες.

Στην αρχή θα δούμε δύο παραδείγματα:

1. Έστω ότι έχουμε το πολυώνυμο x^7-1 επί του $\mathbb{Z}_2$. Με απλή επαλήθευση βλέπουμε ότι η ανάλυσή του σε γινόμενο αναγώγων παραγόντων είναι η εξής: $x^7-1 = (x+1)(x^3+x+1)(x^3+x^2+1)$. Έστω $\mathcal{C} = \langle\, x^3+x+1 \,\rangle$ ο κυκλικός κώδικας με γενήτορα πολυώνυμο x^3+x+1. Τότε ένας γεννήτορας πίνακας είναι ο $\mathrm{G} = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}$ και ένας πίνακας ελέγχου ισοτιμίας για τον κώδικα $\mathcal{C}$ είναι ο πίνακας $\mathrm{P} = \begin{pmatrix} 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$ καθότι ισχύει $\mathrm{GP}^t = \mathbf{0}$. Όπως παρατηρούμε οι στήλες του πίνακα ελέγχου ισοτιμίας αναπαριστούν όλους τους αριθμούς από το 1 έως το $7 = 2^3-1$ σε δυαδική μορφή. Επομένως ο κώδικας $\mathcal{C}$ είναι ισοδύναμος με τον κώδικα Hamming $\mathcal{H}(3,\,2)$, ο οποίος έχει πίνακα ελέγχου ισοτιμίας τον πίνακα $\mathrm{H} = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$ (βλέπε Παράδειγμα $3.1.2_2$).

Εδώ πρέπει να επισημάνουμε ότι ο κώδικας $\mathcal{H}(3,\,2)$ δεν είναι κυκλικός (μπορείτε να ελέγξετε ότι το διάνυσμα $\mathbf{c} = 1000011$ είναι μια (κωδικο)λέξη του $\mathcal{H}(3,\,2)$, ενώ η λέξη 1100001 δεν ανήκει στον $\mathcal{H}(3,\,2)$.

Ας δούμε το προηγούμενο παράδειγμα με τον τρόπο που αναφέρεται στη σελίδα 122. Έστω ω μια πρωταρχική 7^{η} εβδόμη ρίζα της μονάδας επί του $\mathbb{Z}_2$, η οποία μηδενίζει το πολυώνυμο x^3+x+1. Η ω βρίσκεται στο σώμα ριζών του x^3+x+1, έστω $\mathbb{E}$. Το σώμα $\mathbb{E}$ περιέχει $2^3 = 8$ το πλήθος στοιχεία (γιατί;). Επίσης επειδή η ω είναι πρωταρχική ρίζα της μονάδας όλες οι δυνάμεις $\omega,\, \omega^2,\, \ldots,\, \omega^7 = \omega^0 = 1$, είναι διακεκριμένες και ανήκουν στο $\mathbb{E}$. Επομένως τα μη μηδενικά στοιχεία του $\mathbb{E}$ είναι οι δυνάμεις του ω. Αν επιλέξουμε μια βάση του $\mathbb{E}$ ως προς το $\mathbb{Z}_2$, τότε αυτή

θα περιέχει τρία στοιχεία. Έστω $[\omega^j]$ το διάνυσμα στήλη των συντελεστών στην έκφραση του ω^j ως γραμμικού συνδυασμού των στοιχείων αυτής της βάσης με συντελεστές από το σώμα $\mathbb{Z}_2$. Τότε ο πίνακας $\mathrm{H} = \begin{pmatrix} [\omega^0] & [\omega^1] & \cdots & [\omega^6] \end{pmatrix}$ είναι ένας 3×7 πίνακας και οι στήλες του παριστούν όλους τους αριθμούς από το 1 έως το 7 σε δυαδική μορφή, άρα αποτελεί τον πίνακα ελέγχου ισοτιμίας ενός Hamming κώδικα, ο οποίος είναι ο κυκλικός κώδικας $\mathcal{C} = \langle x^3 + x + 1 \rangle$.

2. Στο Παράδειγμα 2.6.22 είχαμε κατασκευάσει όλους τους κυκλικούς κώδικες επί του $\mathbb{Z}_3$ μήκους τέσσερα. Από αυτούς οι κώδικες με γεννήτορες πίνακες $\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}$ $\begin{pmatrix} -1 & 0 & 1 & 0 \\ 0 & -1 & 0 & 1 \end{pmatrix}$ έχουν διάσταση ίση με 2 και ελάχιστη απόσταση το πολύ ίση με 2 (γιατί;).

Ένας τριαδικός Hamming κώδικας μήκους 4 έχει παραμέτρους $[n = (3^2 - 1)/(3-1) = 4,\ k = 4-2 = 2,\ d = 3]$. Επομένως δεν μπορεί να είναι κυκλικός.

Μετά από τα παραδείγματα αυτά είμαστε σε θέση να δούμε τη γενική περίπτωση.

Θεώρημα 3.1.8. *Οι δυαδικοί Hamming κώδικες $\mathcal{H}(r, 2)$ είναι ισοδύναμοι με κυκλικούς κώδικες.*

Απόδειξη. Ως γνωστόν ένας Hamming κώδικες $\mathcal{H}(r, 2)$ έχει παραμέτρους $[n = 2^r - 1,\ k = 2^r - 1 - r,\ d = 3]$ πίνακα ελέγχου ισοτιμίας του οποίου οι στήλες αναπαριστούν όλους τους αριθμούς από το 1 έως το $2^r - 1$. Έστω τώρα ω μια $n-$οστή πρωταρχική ρίζα της μονάδας ($n = 2^r - 1$) επί του $\mathbb{Z}_2$. Το σώμα ριζών της ω, έστω $\mathbb{E}$, αποτελείται από $n + 1 = 2^r$ το πλήθος στοιχεία και είναι διάστασης r ως διανυσματικός χώρος επί του $\mathbb{Z}_2$. Έστω $m_\omega(x)$ το ελαχίστο πολυώνυμο της ω, το σώμα $\mathbb{E}$ είναι επίσης το σώμα ριζών του πολυωνύμου $m_\omega(x)$. Επειδή η ω είναι πρωταρχική ρίζα της μονάδας τα μη μηδενικά στοιχεία του $\mathbb{E}$ είναι οι δυνάμεις της ω. Αν συμβολίζουμε με $[\omega^j]$ το διάνυσμα στήλη των συντελεστών στην έκφραση της ω^j για $j = 0, \ldots, n-1$ ως γραμμικού συνδυασμού των στοιχείων μιας βάσης με συντελεστές από το σώμα $\mathbb{Z}_2$, τότε ο πίνακας $\mathrm{H} = \begin{pmatrix} [\omega^0] & [\omega^1] & \cdots & [\omega^{n-1}] \end{pmatrix}$ είναι ένας $r \times n$ πίνακας και οι στήλες του παριστούν όλους τους αριθμούς από το 1 έως το n σε δυαδική μορφή, άρα αποτελεί τον πίνακα ελέγχου ισοτιμίας ενός Hamming κώδικα, ο οποίος είναι ο κυκλικός κώδικας $\mathcal{C} = \langle m_\omega(x) \rangle$. (Βλέπε τη συζήτηση στη σελίδα 122).

□

Στην περίπτωση που έχουμε έναν $q-$αδικό Hamming κώδικα $\mathcal{H}(r, q)$ με $q \neq 2$, όπως είδαμε και στο παράδειγμα προηγουμένως, ο κώδικας δεν είναι κατ' ανάγκη ισοδύναμος με έναν κυκλικό κώδικα. Το επόμενο θεώρημα δίνει μια ικανή συνθήκη για να είναι ένας κώδικας Hamming ισοδύναμος με έναν κυκλικό κώδικα.

Θεώρημα 3.1.9. *Έστω ο $q-$αδικός Hamming κώδικας $\mathcal{H}(r,\, q)$. Υποθέτουμε ότι μ.κ.δ.$(r,\, q-1) = 1$, τότε ο $\mathcal{H}(r,\, q)$ είναι ισοδύναμος με έναν κυκλικό κώδικα.*

Απόδειξη. Ο κώδικας $\mathcal{H}(r,\, q)$ έχει παραμέτρους $[n = (q^r-1)/(q-1),\, k = (q^r-1)/(q-1) - r,\, d = 3]$. Έστω $\mathbb{E}$ το σώμα ριζών του πολυωνύμου $x^n - 1$ επί του $\mathbb{F}_p$. Υποθέτουμε ότι το $\mathbb{E}$ έχει q^s το πλήθος στοιχεία. Έστω ω μια $n-$οστη πρωταρχική ρίζα της μονάδας τότε εφ' ενός η τάξη της ως στοιχείο της πολλαπλασιαστικής ομάδας του $\mathbb{E}$ είναι ίση με n και ο n διαιρεί τον $q^s - 1$, αφ' ετέρου ο s είναι ο μικρότερος θετικός ακέραιος ώστε η ω να ανήκει σε ένα σώμα με q^s το πλήθος στοιχεία. Δηλαδή έχουμε ότι ο $n = (q^r-1)/(q-1)$ διαιρεί τον q^s-1 και ο s είναι ο μικρότερος θετικός ακέραιος με αυτή την ιδιότητα. Επειδή $(q^r-1)/(q-1) > q^{r-1} - 1$ και $(q^r-1)/(q-1)$ διαιρεί τον $q^r - 1$ έχουμε ότι αναγκαστικά $s = r$. Δηλαδή το σώμα ριζών $\mathbb{E}$ του πολυωνύμου $x^n - 1$ έχει q^r το πλήθος στοιχεία. Αν, όπως προηγουμένως, συμβολίζουμε με $[\omega^j]$ το διάνυσμα στήλη των συντελεστών στην έκφραση της ω^j για $j = 0, \ldots, n-1$ ως γραμμικού συνδυασμού των στοιχείων μιας βάσης με συντελεστές από το σώμα $\mathbb{F}_p$, τότε ο πίνακας $\mathrm{H} = \begin{pmatrix} [\omega^0] & [\omega^1] & \cdots & [\omega^{n-1}] \end{pmatrix}$ είναι ένας $r \times n$ πίνακας. Σκοπός μας είναι να δείξουμε ότι ο κυκλικός κώδικας $\mathcal{C}$, που έχει ως πίνακα ελέγχου ισοτιμίας τον πίνακα H, έχει τις ίδιες παραμέτρους με τον κώδικα $\mathcal{H}(r,\, q)$.

Ανά δύο οι στήλες του πίνακα H είναι γραμμικά ανεξάρτητες. Πράγματι, οι στήλες $[\omega^i]$ και $[\omega^j]$ είναι γραμμικά εξαρτημένες αν και μόνο αν η μια είναι πολλαπλάσιο της άλλης με ένα στοιχείο από το $\mathbb{F}_p$. Αν και μόνο αν $\omega^i \cdot \omega^j = \omega^{i-j} \in \mathbb{F}_p$. Αλλά ένα μη μηδενικό στοιχείο a του $\mathbb{E}$ ανήκει στο $\mathbb{F}_p$ αν και μόνο αν $a^{q-1} = 1$. Επομένως οι δύο στήλες $[\omega^i]$ και $[\omega^j]$ είναι γραμμικά εξαρτημένες αν και μόνο αν $\omega^{(i-j)(q-1)} = 1$. Η ω είναι μια πρωταρχική $n-$οστη ρίζα της μονάδος, άρα $\omega^{(i-j)(q-1)} = 1$ αν και μόνο αν $(i-j)(q-1) \equiv 0 \mathrm{mod} n$. Η τελευταία σχέση με την προϋπόθεση ότι μ.κ.δ.$(r,\, q-1) = 1$ ισχύει (δες την παρατήρηση μετά το τέλος της απόδειξης) μόνο αν $i = j$. Άρα αποδείξαμε ότι ανά δύο οι στήλες του πίνακα H είναι γραμμικά ανεξάρτητες. Επομένως ο κυκλικός κώδικας $\mathcal{C}$ έχει μήκος ίσο με $n = (q^r-1)/(q-1)$, διάσταση $k \geq (q^r-1)/(q-1) - r$ και ελάχιστη απόσταση $d \geq 3$ (βλέπε Πρόταση 2.2.27). Τώρα από το Θεώρημα 1.5.8 έπεται εύκολα ότι $k = (q^r-1)/(q-1) - r$ και $d = 3$, οπότε η απόδειξη τελείωσε.

□

Παρατηρήσεις 3.1.10. 1. Στην προηγούμενη απόδειξη ισχυριστήκαμε ότι ισχύει $(i-j)(q-1) \equiv 0 \mathrm{mod} n$ με την προϋπόθεση ότι μ.κ.δ.$(r,\, q-1) = 1$ μόνο αν $i = j$.

Πράγματι, θα αποδείξουμε την εξής απλή άσκηση στη Θεωρία αριθμών.

Έστω q δύναμη πρώτου αριθμού, r θετικός ακέραιος και $n = (q^r - 1)/(q - 1)$, τότε ισχύει $\mu.\kappa.\delta.\,(r, q-1) = 1$ αν και μόνο αν $\mu.\kappa.\delta.\,(n, q-1) = 1$.

Έχουμε ότι $n = (q^r - 1)/(q - 1) = 1 + q + q^2 + \cdots + q^{r-1}$ και ο $q - 1$ διαιρεί τον $q^i - 1$ για κάθε $i = 0, 1, \ldots, r - 1$, δηλαδή υπάρχουν ακέραιοι s_i έτσι ώστε $q^i = (q - 1)s_i + 1$. Επομένως έχουμε ότι $n = ((q-1)s_0+1)+((q-1)s_1+1)+\cdots+((q-1)s_{r-1}+1) = (q-1)s+r$. Άρα $\mu.\kappa.\delta.\,(r, q-1) = 1$ αν και μόνο αν $\mu.\kappa.\delta.\,(n, q-1) = 1$.

Επανερχόμενοι τώρα στα προηγούμενα, με την προϋπόθεση ότι $\mu.\kappa.\delta.\,(r, q-1) = 1$ (δηλαδή ότι $\mu.\kappa.\delta.\,(n, q-1) = 1$) έχουμε ότι $(i - j)(q - 1) \equiv 0 \bmod n$ συνεπάγεται ότι $i = j$ δεδομένου ότι το n είναι η τάξη της ρίζας ω.

2. Στο προηγούμενο Παράδειγμα 2 είχαμε δεί ότι ο τριαδικός Hamming κώδικας $\mathcal{H}(2, 3)$ δεν είναι ισοδύναμος με έναν κυκλικό κώδικα. Το αποτέλεσμα αυτό συνάδει με το προηγούμενο θεώρημα καθότι $\mu.\kappa.\delta.\,(r = 2, q - 1 = 2) \neq 1$, αλλά δεν απορρέει ως αποτέλεσμα από το θεώρημα, διότι στο θεώρημα διατυπώνεται (μόνο) μια ικανή συνθήκη για να είναι ένας Hamming κώδικας κυκλικός.

3.1.4 Ασκήσεις

1. Με τη βοήθεια του Hamming κώδικα $\mathcal{H}(3, 2)$ να αποκωδικοποιήσετε τις λέξεις 1111000 και 1111111.

2. Με τη βοήθεια του Hamming κώδικα $\mathcal{H}(3, 3)$ αποκωδικοποιήσετε τις λέξεις 1111001122201 και 0012200112202.

3. Εφαρμόζοντας στοιχειώδεις μετσχηματισμούς στον πίνακα ελέγχου ισοτιμίας του κώδικα $\mathcal{H}(3, 2)$ να τον φέρετε στη μορφή $[\mathrm{A}\ \mathrm{I}_3]$, κατόπιν υπολογίστε έναν γεννήτορα πίνακα του $\mathcal{H}(3, 2)$.

4. Έστω $\widehat{\mathcal{H}(r, 2)}$ ο κώδικας που προκύπτει από την προσθήκη ενός ψηφίου ελέγχου ισοτιμίας στον κώδικα Hamming $\mathcal{H}(r, 2)$. Εξετάστε αν η δυνατότητα διόρθωσης λαθών αυξάνουν με τον νέο κώδικα. Τι συμβαίνει με τη δυνατότητα ανίχνευσης λαθών;

5. Υποθέτουμε ότι έχουμε έναν συμμετρικό δυαδικό δίαυλο επικοινωνίας. Δείξτε ότι η πιθανότητα σωστής αποκωδικοποίησης με τη βοήθεια του συνδρόμου, είναι ίδια είτε χρησιμοποιήσουμε τον κώδικα Hamming $\mathcal{H}(r, 2)$, είτε

χρησιμοποιήσουμε τον κώδικα $\widehat{\mathcal{H}(r,\,2)}$ που προκύπτει από την προσθήκη ενός ψηφίου ελέγχου ισοτιμίας στον κώδικα Hamming $\mathcal{H}(r,\,2)$.

6. Να γενικεύσετε την προηγούμενη άσκηση στην περίπτωση ένος (τυχαίου) δυαδικού τέλειου κώδικα.

7. Δείξτε ότι αν q είναι μια δύναμη ενός πρώτου αριθμού και $3 \leq n \leq q+1$, τότε $A_q(n,\,3) = q^{n-2}$.

8. Έχοντας υπ' όψη ότι Hamming κώδικες είναι τέλειοι, υπολογίστε τον αριθμό των (κωδικο)λέξεων βάρους 3 στον κώδικα $\mathcal{H}(r,\,2)$. (Συγκεκριμένα δείξτε ότι ο αριθμός αυτός είναι ίσος με $(2^r-1)(2^{r-1}-1)/3$

9. Να υπολογίσετε τον απαριθμητή βάρους του κώδικα $\mathcal{H}(3,\,2)$.

10. Να υπολογίσετε το πολυώνυμο γεννήτορα του (ισοδυνάμου) κυκλικού Hamming κώδικα $\mathcal{H}(3,\,2)$.

3.2 Κώδικες Golay

Οι κώδικες Golay αποτελούν μια πολύ ειδική κατηγορία κωδίκων, η οποία είναι από τις πλέον σημαντικές κατηγορίες κωδίκων που έχουν επινοηθεί. Υπάρχουν τέσσερεις κώδικες Golay, δύο από αυτούς είναι δυαδικοί και δύο τριαδικοί. Όλοι είναι γραμμικοί κώδικες. Δύο από αυτούς είναι κυκλικοί και τέλειοι, ενώ οι άλλοι δύο μπορούν να προκύψουν ως επεκτάσεις αυτών.

Οι κώδικες αυτοί επινοήθηκαν το 1948 από τον Golay και χρησιμοποιήθηκαν την περίοδο 1979 - 1981 από το διαστημόπλοιο Voyager για την αποστολή εγχρώμων φωτογραφιών στη γη από τους πλανήτες Δία και Κρόνο.

Η εισαγωγή των αυτών κωδίκων έγινε από τον Golay παρουσιάζοντας τους αντίστοιχους γεννήτορες πίνακες. Ο τρόπος αυτός ορισμού των δεν δίνει καμία ένδειξη για τον λόγο που χρησιμοποιήθηκαν αυτοί οι συγκεκριμένοι πίνακες. Κατόπιν, λόγω του μεγάλου ενδιαφέροντος που παρουσιάζουν, επινοήθηκαν διάφοροι άλλοι τρόποι ορισμού των οι οποίοι όχι μόνο αποδεικνύουν με σύντομο και κομψό τρόπο τις ιδιότητες των κωδίκων Golay, αλλά και την μοναδικότητά τους.

3.2.1 Δυαδικοί κώδικες Golay

Έστω ο 12×12 πίνακας με στοιχεία από το $\mathbb{Z}_2$

$$\mathrm{A} = \begin{pmatrix} \cdot & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & \cdot & 1 & 1 & 1 & \cdot & \cdot & \cdot & 1 & \cdot \\ 1 & 1 & \cdot & 1 & 1 & 1 & \cdot & \cdot & \cdot & 1 & \cdot & 1 \\ 1 & \cdot & 1 & 1 & 1 & \cdot & \cdot & \cdot & 1 & \cdot & 1 & 1 \\ 1 & 1 & 1 & 1 & \cdot & \cdot & \cdot & 1 & \cdot & 1 & 1 & \cdot \\ 1 & 1 & 1 & \cdot & \cdot & \cdot & 1 & \cdot & 1 & 1 & \cdot & 1 \\ 1 & 1 & \cdot & \cdot & \cdot & 1 & \cdot & 1 & 1 & \cdot & 1 & 1 \\ 1 & \cdot & \cdot & \cdot & 1 & \cdot & 1 & 1 & \cdot & 1 & 1 & 1 \\ 1 & \cdot & \cdot & 1 & \cdot & 1 & 1 & \cdot & 1 & 1 & 1 & \cdot \\ 1 & \cdot & 1 & \cdot & 1 & 1 & \cdot & 1 & 1 & 1 & \cdot & \cdot \\ 1 & 1 & \cdot & 1 & 1 & \cdot & 1 & 1 & 1 & \cdot & \cdot & \cdot \\ 1 & \cdot & 1 & 1 & \cdot & 1 & 1 & 1 & \cdot & \cdot & \cdot & 1 \end{pmatrix},$$

όπου στη θέση των $\cdot$ είναι μηδενικά.

Ορισμός 3.2.1. *Ο γραμμικός κώδικας με γεννήτορα πίνακα τον πίνακα* $\mathrm{G} = [\mathrm{I}_{12}\, \mathrm{A}]$ *λέγεται (επεκταμένος) κώδικας Golay και συμβολίζεται* $\mathcal{G}_{24}$.

Πρόταση 3.2.2. *1. Ο κώδικας* $\mathcal{G}_{24}$ *είναι αυτοδυϊκός.*

2. Ο πίνακας $[\mathrm{A}\, \mathrm{I}_{12}]$ *είναι επίσης ένας γεννήτορας πίνακας του* $\mathcal{G}_{24}$.

Απόδειξη. Δεν είναι δύσκολο να δούμε ότι ανά δύο οι γραμμές του γεννήτορα πίνακα $\mathrm{G} = [\mathrm{I}_{12}\, \mathrm{A}]$ είναι κάθετες μεταξύ τους. Δηλαδή $\mathrm{G} \cdot \mathrm{G}^t = \mathbf{0}$. Από την Πρόταση 2.2.12 και το Θεώρημα 2.2.13 έπεται ότι $\mathcal{G}_{24} = \mathcal{G}_{24}^{\perp}$.

Παρατηρούμε ότι ο πίνακας A είναι συμμετρικός, οπότε από το Θεώρημα 2.2.17 έπεται ότι ο πίνακας $[\mathrm{A}\, \mathrm{I}_{12}]$ είναι επίσης ένας γεννήτορας πίνακας του $\mathcal{G}_{24}$. □

Λήμμα 3.2.3. *Το βάρος κάθε (κωδικο)λέξης στον κώδικα* $\mathcal{G}_{24}$ *είναι πολλαπλάσιο του 4, αλλά δεν ισούται με 4.*

Απόδειξη. Παρατηρούμε ότι το βάρος κάθε γραμμήσ̈του γεννήτορα πίνακα G είναι πολλαπλάσιο του 4. Έστω $\mathbf{r}$ και $\mathbf{s}$ δύο γραμμές του G, από την Πρόταση 1.2.10 έχουμε ότι $w(\mathbf{r}+\mathbf{s}) = w(\mathbf{r}) + w(\mathbf{s}) - 2w(\mathbf{r} \cap \mathbf{s})$. Αλλά προηγουμένως έχουμε αποδείξει ότι οι γραμμές του πίνακα G είναι ανά δύο κάθετες, δηλαδή $w(\mathbf{r} \cap \mathbf{s}) = 0 \bmod (2)$. Επομένως και το $w(\mathbf{r}+\mathbf{s})$ είναι πολλαπλάσιο του 4.

Επειδή ο κώδικας είναι δυαδικός, κάθε (κωδικο)λέξη είναι άθροισμα γραμμών του πίνακα G. Άρα έχει βάρος πολλαπλάσιο του 4.

Υποθέτουμε τώρα ότι υπάρχει μια (κωδικο)λέξη $\mathbf{c} = c_1\, c_2 \cdots c_{12}\, c_{13} \cdots c_{24}$ με βάρος ίσο με 4. Αν χωρίσουμε τη $\mathbf{c}$ σε δύο τμήματα $\mathbf{a} = c_1\, c_2 \cdots c_{12}$ και $\mathbf{b} = c_{13} \cdots c_{24}$, τότε διακρίνουμε τις εξής περιπτώσεις.

1. $w(\mathbf{a}) = 0$ και $w(\mathbf{b}) = 4$. Η περίπτωση αυτή είναι αδύνατη, καθότι από τον γεννήτορα πίνακα $[\mathrm{I}_{12}\,\mathrm{A}]$ έπεται ότι μόνο η μηδενική λέξη έχει τους πρώτους 12 χαρακτήρες όλους ίσους με 0.

2. $w(\mathbf{a}) = 4$ και $w(\mathbf{b}) = 0$. Όμοια η περίπτωση αυτή είναι αδύνατη, καθότι από τον γεννήτορα πίνακα $[\mathrm{A}\,\mathrm{I}_{12}]$ έπεται ότι μόνο η μηδενική λέξη έχει τους 12 τελευταίους χαρακτήρες όλους ίσους με 0.

3. $w(\mathbf{a}) = 1$ και $w(\mathbf{b}) = 3$. Η περίπτωση αυτή είναι αδύνατη, καθότι από τον γεννήτορα πίνακα $[\mathrm{I}_{12}\,\mathrm{A}]$ έπεται ότι η λέξη $\mathbf{c}$ πρέπει να είναι μια γραμμή του, αλλά καμία γραμμή του γεννήτορα πίνακα δεν έχει βάρος ίσο με 4.

4. $w(\mathbf{a}) = 3$ και $w(\mathbf{b}) = 1$. Όμοια η περίπτωση αυτή είναι αδύνατη, καθότι από τον γεννήτορα πίνακα $[\mathrm{A}\,\mathrm{I}_{12}]$ έπεται ότι η λέξη $\mathbf{c}$ πρέπει να είναι μια γραμμή του, αλλά καμία γραμμή του γεννήτορα πίνακα δεν έχει βάρος ίσο με 4.

   Απομένει μόνο η περίπτωση

5. $w(\mathbf{a}) = 2$ και $w(\mathbf{b}) = 2$. Στη περίπτωση αυτή έπεται ότι η λέξη $\mathbf{c}$ πρέπει να είναι το άθροισμα δύο γραμμών του πίνακα $[\mathrm{I}_{12}\,\mathrm{A}]$. Αλλά το άθροισμα δύο οποιωνδήποτε γραμμών του πίνακα A δεν έχει βάρος ίσον με 2.

   Άρα τελικά δεν υπάρχει $\mathbf{c} \in \mathcal{G}_{24}$ με βάρος ίσο με 4.

□

Από τα προηγούμενα έπεται το ακόλουθο θεώρημα.

Θεώρημα 3.2.4. *Ο κώδικας $\mathcal{G}_{24}$ είναι ένας* $[24, 12, 8]$ *γραμμικός κώδικας.*

Απόδειξη. Η απόδειξη είναι άμεση από τα προηγούμενα αρκεί να παρατηρήσουμε ότι η δεύτερη γραμμή του γεννήτορα πίνακα $\mathrm{G} = [\mathrm{I}_{12}\,\mathrm{A}]$ έχει βάρος ίσο με 8.

□

Παρατηρήσεις 3.2.5. 1. Στην Πρόταση ;; ο έλεγχος καθετότητας ανα δύο των γραμμών του γεννήτορα πίνακα $\mathrm{G} = [\mathrm{I}_{12}\,\mathrm{A}]$ δεν είναι δύσκολος, αλλά είναι χρονοβόρος. Παρατηρούμε ότι το δεύτερο ήμισυ κάθε γραμμής, από την τρίτη έως και τη δωδέκατη, προέρχεται από μια κυκλική μετάθεση των στοιχείων του δεύτερου ήμισυ της δεύτερης γραμμής. Επομένως για τον έλεγχο της καθετότητας δύο γραμμών του πίνακα είναι αρκετό να ελέγξουμε την καθετότητα μόνο της πρώτης και δεύτερης γραμμής ως προς τις γραμμές του πίνακα.

2. Ο γεννήτορας πίνακας $\mathrm{G} = [\mathrm{I}_{12}\,\mathrm{A}]$ δεν είναι ο πίνακας που αρχικά επινοήθηκε από τον Golay, αλλά ένας πίνακας που δίνει έναν (ισοδύναμο) [24, 12, 8] κώδικα Golay.

Αν από κάθε στοιχείο του κώδικα $\mathcal{G}_{24}$ διαγράψουμε τον τελευταίο χαρακτήρα, τότε επιτυγχάνουμε μια σύμπτυξη του κώδικα σε έναν άλλο κώδικα $\mathcal{G}_{23}$ με παραμέτρους $(23,\, 2^{12},\, 7)$, (ο οποίος προς το παρόν δεν γνωρίζουμε αν είναι γραμμικός). Ο κώδικας $\mathcal{G}_{23}$ είναι ο δεύτερος δυαδικός κώδικας Golay και είναι τέλειος. Πράγματι, έχουμε ότι $2^{12}\big[\,1+23+\binom{23}{2}+\binom{23}{3}\,\big] = 2^{23}$, οπότε από την πρόταση 1.5.12 έχουμε ότι ο $\mathcal{G}_{23}$ είναι τέλειος.

Παρατήρηση 3.2.6. Αντί να διαγράψουμε τον τελευταίο χαρακτήρα κάθε (κωδικο)λέξης του $\mathcal{G}_{24}$ για να πάρουμε τον $\mathcal{G}_{23}$, θα μπορούσαμε να διαγράψουμε τον χαρακτήρα από μια συγκεκριμένη θέση σε όλες τις (κωδικο)λέξεις του $\mathcal{G}_{24}$ και να πάρουμε έναν ισοδύναμο κώδικα προς τον $\mathcal{G}_{23}$ (γιατί;).

Επίσης θα μπορούσαμε να πάρουμε τον $\mathcal{G}_{24}$ σαν επέκταση του $\mathcal{G}_{23}$ προσθέτοντας ένα στοιχείο ελέγχου ισοτιμίας οπότε από το Θεώρημα 1.4.9 δεν έχει σημασία ποιόν από τους $\mathcal{G}_{24}$ ή $\mathcal{G}_{23}$ θα ορίσουμε πρώτα.

Ο κώδικας $\mathcal{G}_{24}$ διορθώνει τρία λάθη. Αν θελήσουμε να πραγματοποιήσουμε αποκωδικοποίηση με την βοήθεια των συνδρόμων, τότε πρέπει να υπολογίσουμε $\frac{2^{24}}{2^{12}} = 2^{12} = 4096$ το πλήθος σύνδρομα. Εκμεταλευόμενοι τη δομή του κώδικα μπορούμε να περιορίσουμε κατά πολύ τον αριθμό των απαιτουμένων συνδρόμων για την αποκωδικοποίηση μιας λέξης.

Έστω ότι ελήφθει η λέξη $\mathbf{x}$ και ότι κατά την αποστολή υπεισήλθαν 3 το πολύ λάθη, δηλαδή το διάνυσμα λάθους $\mathbf{e}$ έχει βάρος $w(\mathbf{e}) \leq 3$.

Ο κώδικας $\mathcal{G}_{24}$ είναι αυτοδυϊκός, επομένως οι πίνακες $\mathrm{G} = [\mathrm{I}_{12}\,\mathrm{A}]$ και $\mathrm{C} = [\mathrm{A}\,\mathrm{I}_{12}]$ είναι ταυτόχρονα και γεννήτορες και πίνακες ελέγχου ισοτιμίας. Ο υπολογισμός του συνδρόμου της λέξης $\mathbf{x}$ τόσο με την βοήθεια του πίνακα G όσο και με την βοήθεια του πίνακα C μας επιτρέπει να υπολογίσουμε το διάνυσμα λάθους σχετικά εύκολα.

Κατ' αρχήν παρατηρούμε ότι το άθροισμα τρίων ή λιγότερο το πλήθος γραμμών του πίνακα A έχει βάρος τουλάχιστον ίσο με 5 (δες τη μορφή του πίνακα A).

Θεωρούμε ότι το $\mathbf{e}$ αποτελείται από δύο τμήματα, δηλαδή $\mathbf{e} = \mathbf{e}_1\mathbf{e}_2$, όπου το κάθε ένα από τα $\mathbf{e}_i$ είναι μήκους 12. Τότε έχουμε $\mathbf{x}\mathrm{G}^{\perp} = \mathbf{e}\mathrm{G}^{\perp} = \mathbf{e}_1 + \mathbf{e}_2\mathrm{A}$ και $\mathbf{x}\mathrm{C}^{\perp} = \mathbf{e}\mathrm{C}^{\perp} = \mathbf{e}_1\mathrm{A} + \mathbf{e}_2$.

Από τις προηγούμενες σχέσεις υπολογίζουμε τα βάρη των συνδρόμων $\mathbf{x}\mathrm{G}^{\perp} = \mathbf{e}\mathrm{G}^{\perp}$ και $\mathbf{x}\mathrm{C}^{\perp} = \mathbf{e}\mathrm{C}^{\perp}$.

Διακρίνουμε περιπτώσεις:

(i) $w(\mathbf{e}\mathrm{G}^{\perp}) \geq 5$ και $w(\mathbf{e}\mathrm{C}^{\perp}) \leq 3$

(ii) $w(\mathbf{e}\mathrm{G}^{\perp}) \leq 3$ και $w(\mathbf{e}\mathrm{C}^{\perp}) \geq 5$

$(iiii)$ $w(\mathbf{e}\mathrm{G}^{\perp}) \geq 5$ και $w(\mathbf{e}\mathrm{C}^{\perp}) \geq 5$

Αν έχουμε την πρώτη περίπτωση, τότε από τις προηγούμενες σχέσεις έπεται ότι αναγκαστικά το πρώτο τμήμα $\mathbf{e}_1$ στο διάνυσμα λάθους $\mathbf{e}$ είναι ίσο με το μηδενικό διάνυσμα ($\mathbf{e}_1 = \mathbf{0}$), οπότε από τη σχέση $\mathbf{x}\mathrm{C}^{\perp} = \mathbf{e}\mathrm{C}^{\perp} = \mathbf{e}_1\mathrm{A} + \mathbf{e}_2$ εύκολα έπεται ότι $\mathbf{e} = \mathbf{0}\mathbf{e}_2 = \mathbf{0}(\mathbf{x}\mathrm{C}^{\perp})$.

Όμοια αν έχουμε την δεύτερη περίπτωση, τότε έπεται ότι $\mathbf{e} = \mathbf{e}_1\mathbf{0} = (\mathbf{x}\mathrm{G}^{\perp})\mathbf{0}$.

Αν έχουμε την τρίτη περίπτωση τότε έπεται ότι τόσο το τμήμα $\mathbf{e}_1$, όσο και το τμήμα $\mathbf{e}_2$ είναι μη μηδενικά. Αυτό σημαίνει ότι έχουν υπεισέλθει λάθη τόσο στις πρώτες 12 θέσεις, όσο και στις υπόλοιπες 12 θέσεις. Μάλιστα δε αν έχει υπεισέλθει ένα λάθος στο πρώτο τμήμα, τότε στο δεύτερο έχουν υπεισέλθει το πολύ δύο και αντίστροφα.
Έστω ότι ένα λάθος εμφανίζεται στο πρώτο τμήμα στη θέση i, $i = 1, 2, \ldots, 12$, τότε το $\mathbf{e}_1$ θα ισούται με ένα από τα $\epsilon_i = 0\,0 \cdots 1 \cdots 0$, οπότε υπολογίζοντας τα 12 σύνδρομα $(\mathbf{x} + \epsilon_j\mathbf{0})\mathrm{C}^{\perp} = (\mathbf{e} + \epsilon_j\mathbf{0})\mathrm{C}^{\perp} = (\epsilon_i\mathbf{e}_2 + \epsilon_j\mathbf{0})\mathrm{C}^{\perp} = \epsilon_i\mathrm{A} + \mathbf{e}_2 + \epsilon_j\mathrm{A}$ για $j = 1, 2 \ldots, 12$ εντοπίζουμε τη θέση i του λάθους ως εξής:

Όλα τα παραπάνω σύνδρομα έχουν βάρος τουλάχιστον ίσο με 4 (γιατί;) εκτός από την περίπτωση όπου $i = j$, όπου έχουμε $\epsilon_i\mathrm{A} + \mathbf{e}_2 + \epsilon_i\mathrm{A} = \mathbf{e}_2$ και συνεπώς προσδιορίζουμε τόσο τη θέση του ενός λάθους στο πρώτο τμήμα $\mathbf{e}_1$, όσο και το δεύτερο τμήμα $\mathbf{e}_2$.

Παρόμοια αντιμετωπίζεται η περίπτωση όπου στο πρώτο τμήμα εμφανίζονται δύο λάθη (οπότε στο δεύτερο εμφανίζεται ακριβώς ένα λάθος).

Ανακεφαλαιώνοντας βλέπουμε ότι είναι αρκετός ο υπολογισμός 26 (το πολύ) συνδρόμων για να εντοπίσουμε και να διορθώσουμε μέχρι τρία λάθη με το κώδικα $\mathcal{G}_{24}$.

3.2.2 Τριαδικοί κώδικες Golay

Έστω ο 6×6 πίνακας με στοιχεία από το $\mathbb{Z}_3$

$$\mathrm{B} = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 2 & 2 & 1 \\ 1 & 1 & 0 & 1 & 2 & 2 \\ 1 & 2 & 1 & 0 & 1 & 2 \\ 1 & 2 & 2 & 1 & 0 & 1 \\ 1 & 1 & 2 & 2 & 1 & 0 \end{pmatrix},$$

Ορισμός 3.2.7. *Ο γραμμικός κώδικας με γεννήτορα πίνακα τον πίνακα* $\mathrm{G} = [\mathrm{I}_6\,\mathrm{B}]$ *λέγεται (επεκταμένος) τριαδικός κώδικας Golay και θα συμβολίζεται* $\mathcal{G}_{12}$.

Όπως και στην περίπτωση του δυαδικού κώδικα Golay $\mathcal{G}_{24}$ μπορούμε να αποδείξουμε το ακόλουθο θεώρημα.

Θεώρημα 3.2.8. *1. Ο τριαδικός κώδικας Golay $\mathcal{G}_{12}$ είναι αυτοδυϊκός.*

2. Ο πίνακας $[-\mathrm{B}\,\mathrm{I}_6]$ είναι επίσης ένας γεννήτορας πίνακας του $\mathcal{G}_{12}$.

3. Ο κώδικας $\mathcal{G}_{12}$ είναι ένας $[12, 6, 6]$ κώδικας.

4. Ο τριαδικός κώδικας $\mathcal{G}_{11}$ που προέρχεται από τον $\mathcal{G}_{12}$, όταν διαγράψουμε τον τελευταίο χαρακτήρα από κάθε στοιχείο του $\mathcal{G}_{12}$, είναι ένας $[11, 6, 5]$ τέλειος κώδικας.

Απόδειξη. Η απόδειξη είναι όμοια, όπως στην περίπτωση του $\mathcal{G}_{24}$ και αφίνεται ως άσκηση.

□

Επίσης ο κώδικας $\mathcal{G}_{12}$ προέρχεται από τον κώδικα $\mathcal{G}_{11}$ προσθέτοντας ένα ψηφίο ελέγχου ισοτιμίας.

3.2.3 Οι κώδικες Golay ως κυκλικοί κώδικες

Εδώ θα δούμε πως οι κώδικες $\mathcal{G}_{23}$ και $\mathcal{G}_{11}$ μπορούν να θεωρηθούν κατά ένα φυσιολογικό τρόπο ως κυκλικοί κώδικες.

Πρώτα θα εξετάσουμε την περίπτωση του δυαδικού κώδικα $\mathcal{G}_{23}$. Το μόνο που θα θεωρήσουμε ως δεδομένο είναι η ανάλυση του πολυωνύμου $x^{23}-1 = (x-1)\cdot(x^{11}+x^{10}+x^6+x^5+x^4+x^2+1)\cdot(x^{11}+x^9+x^7+x^6+x^5+x+1) \in \mathbb{Z}_2[x]$ σε γινόμενο αναγώγων πολυωνύμων. Έστω $g_1(x) = x^{11}+x^{10}+x^6+x^5+x^4+x^2+1$ και $g_2(x) = x^{11}+x^9+x^7+x^6+x^5+x+1$, όπως βλέπουμε τα $g_1(x)$ και $g_2(x)$ είναι αμοιβαία πολυώνυμα (βλέπε Παρατήρηση 2.6.26). Επομένως αν $\mathcal{C}_1 = \langle g_1(x)\rangle$ και $\mathcal{C}_2 = \langle g_2(x)\rangle$, τότε οι $\mathcal{C}_1$ και $\mathcal{C}_2$ είναι ισοδύναμοι κώδικες. Από την Πρόταση 2.6.20 έχουμε ότι ο κυκλικός κώδικας $\mathcal{C}_1 = \langle g_1(x)\rangle$ έχει παραμέτρους $[23, 12, ?]$. Ο σκοπός μας τώρα είναι να υπολογίσουμε την ελάχιστη απόστασή του.

Λήμμα 3.2.9. *Έστω $x^p - 1 = (x-1)\cdot g_1(x)\cdot g_2(x) \in \mathbb{Z}_2[x]$, όπου p είναι ένας περιττός πρώτος. Υποθέτουμε ότι οι κυκλικοί κώδικες $\mathcal{C}_1 = \langle g_1(x)\rangle$ και $\mathcal{C}_2 = \langle g_2(x)\rangle$ είναι ισοδύναμοι. Αν $a(x)$ είναι μια (κωδικο)λέξη του $\mathcal{C}_1$ περιττού βάρους, έστω w, τότε $w^2 \geq p$. Αν επιπλέον τα δύο πολυώνυμα $g_1(x)$ και $g_2(x)$ είναι αμοιβαία πολυώνυμα, τότε $w^2 - w + 1 \geq p$.*

Απόδειξη. Επειδή οι κώδικες $\mathcal{C}_1$ και $\mathcal{C}_2$ είναι ισοδύναμοι, υπάρχει μια (κωδικο)λέξη $b(x) \in \mathcal{C}_2$, η οποία έχει και αυτή βάρος ίσο με w. Το πολυώνυμο $a(x)$ είναι πολλαπλάσιο του $g_1(x)$, όμοια το πολυώνυμο $b(x)$ είναι πολλαπλάσιο του $g_2(x)$,

επομένως το πολυώνυμο $a(x)\cdot b(x)$ είναι πολλαπλάσιο του $g_1(x)\cdot g_2(x)$. Άρα το $a(x)\cdot b(x)$ θα είναι ίσο με $\mathbf{0}$ ή ίσο με $g_1(x)\cdot g_2(x)$.
(Υπενθυμίζουμε ότι ο πλλαπλασιασμός γίνεται $(\mathrm{mod}(x^p-1))$.
Επειδή το βάρος w είναι περιττό, έχουμε ότι $w\cdot w = a(1)\cdot b(1) \equiv 1\mathrm{mod}(2)$. Επομένως αναγκαστικά $a(x)\cdot b(x) = g_1(x)\cdot g_2(x) = 1+x+x^2+\cdots+x^{p-1}$. Αλλά το γινόμενο $a(x)\cdot b(x)$ έχει το πολύ w^2 το πλήθος μη μηδενικούς συντελεστές, επομένως $w^2 \geq p$.

Στην περίπτωση που τα $g_1(x)$ και $g_2(x)$ είναι αμοιβαία πολυώνυμα, τότε τα στοιχεία του κώδικα $\mathcal{C}_2 = \langle g_2(x)\rangle$ είναι τα αμοιβαία στοιχεία των στοιχείων του κώδικα $\mathcal{C}_1 = \langle g_1(x)\rangle$ (βλέπε Παρατήρηση $2.6.26_3$). Επομένως αν στη θέση του $b(x)$ παραπάνω πάρουμε το $a(x^{-1})$, τότε έχουμε $a(x)\cdot a(x^{-1}) = 1+x+x^2+\cdots+x^{p-1}$. Από τους w^2 το πλήθος όρους του γινομένου $a(x)\cdot a(x^{-1})$ οι w είναι ίσοι με 1 επομένως το μέγιστο βάρος του $a(x)\cdot a(x^{-1})$ ισουται με w^2-w+1, δηλαδή $w^2-w+1\geq p$.

□

Λήμμα 3.2.10. *Έστω $x^p-1 = (x-1)\cdot g_1(x)\cdot g_2(x)\in\mathbb{Z}_2[x]$, όπου pείναι ένας περιττός πρώτος. Υποθέτουμε ότι τα πολυώνυμα $g_1(x)$ και $g_2(x)$ είναι αμοιβαία. Αν $a(x)$ είναι μια (κωδικο)λέξη του $\mathcal{C} = \langle g_1(x)\rangle$ αρτίου βάρους, έστω w, τότε $w\equiv 0\mathrm{mod}(4)$. Επιπλέον αν $p\neq 7$, τότε $w\neq 4$.*

Απόδειξη. Όπως και στην απόδειξη του προηγουμένου λήμματος έχουμε ότι $a(x)\cdot a(x^{-1}) = 0$ ή $a(x)\cdot a(x^{-1}) = 1+x+x^2+\cdots+x^{p-1}$. Το $a(x)$ είναι αρτίου βάρους, επομένως $a(1)=0$ και συνεπώς $a(x)\cdot a(x^{-1}) = 0$. Υποθέτουμε ότι $a(x) = x^{e_1}+x^{e_2}+\cdots+x^{e_w}$. Τότε $a(x)\cdot a(x^{-1}) = \sum_{i=1}^{w}\sum_{j=1}^{w} x^{e_i-e_j} = 0$ (οι πράξεις γίνονται $(\mathrm{mod}(x^p-1))$. Στο προηγούμενο άθροισμα έχουμε w^2 το πλήθος προσθεταίους. Στην περίπτωση όπου $i=j$ ο αντίστοιχος προσθεταίος είναι ίσος με 1, υπάρχουν w το πλήθος τέτοιοι προσθεταίοι, και επειδή το w είναι άρτιος το αθροισμά τους είναι ίσο με $0\mathrm{mod}(2)$. Οι υπόλοιποι w^2-w το πλήθος προσθεταίοι είναι της μορφής $x^{e_i-e_j}$ με $i\neq j$ και πρέπει να διαγράφονται ανά ζεύγη. Αλλά αν $x^{e_i-e_j} = x^{e_k-e_\ell}$, τότε και $x^{e_j-e_i} = x^{e_\ell-e_k}$. Αυτό σημαίνει ότι οι προσθεταίοι αυτοί στο παραπάνω άθροισμα διαγράφονται άνα τετράδες. Δηλαδή $w^2-w\equiv 0\mathrm{mod}(4)$, από όπου έπεται $w\equiv 0\mathrm{mod}(4)$.

Υποθέτουμε τώρα ότι $w=4$. Άνευ βλάβης της γενικότητας (επειδή ο κώδικας είναι κυκλικός) μπορούμε να υποθέσουμε ότι $a(x) = x^k+x^j+x^i+1$ με $1<k,\,j,\,i<p$. Απο τη σχέση $a(x)\cdot a(x^{-1}) = (x^k+x^j+x^i+1)(x^{-k}+x^{-j}+x^{-i}+1) = 0$ έπεται ότι οι εκθέτες του γινομένου $(x^k+x^j+x^i+1)(x^{-k}+x^{-j}+x^{-i}+1)$ πρέπει να σχηματίζουν ζεύγη των οποίων τα μέλη να είναι ισότιμα $\mathrm{mod}(p)$. Εκτελώντας τις πράξεις, λόγω συμμετρίας, είναι αρκετό να εξετάσουμε κατά πόσο το i είναι ισότιμο $\mathrm{mod}(p)$ με το $j-k$ ή με το $-j$ ή με το $j-i$.

i) Υποθέτουμε ότι $i \equiv (j-k)\mathrm{mod}(p)$, τότε όμως έχουμε $k \equiv (j-i)\mathrm{mod}(p)$, οπότε αναγκαστικά $j \equiv \pm(i-k)\mathrm{mod}(p)$. Από την πρώτη και τρίτη σχέση έπεται ότι $2k \equiv 0\mathrm{mod}(p)$ ή $2i \equiv 0\mathrm{mod}(p)$. Αυτό είναι αδύνατον, διότι έχει υποτεθεί ότι ο p είναι περιττός πρώτος.

ii) Υποθέτουμε ότι $i \equiv -j\mathrm{mod}(p)$. Έχοντας αποκλείσει δυνατότητες που εμφανίζονται στην πρώτη περίπτωση, έπεται ότι $k \equiv i - k\mathrm{mod}(p)$ ή $k \equiv j - k\mathrm{mod}(p)$. Υποθέτουμε ότι ισχύει η πρώτη σχέση (όμοια εξετάζεται και η δεύτερη), οπότε έχουμε $2k \equiv i\mathrm{mod}(p)$. Τότε όμως αναγκαστικα θα ισχύει και $(i-j) \equiv (j-k)\mathrm{mod}(p)$. Συνδυάζοντας την τελευταία σχέση με τις σχέσεις $i \equiv -j\mathrm{mod}(p)$ και $2k \equiv i\mathrm{mod}(p)$ έχουμε ότι $7k \equiv 0\mathrm{mod}(p)$, δηλαδή $p = 7$.

iii) Υποθέτουμε ότι $i \equiv (j-i)\mathrm{mod}(p)$. Έχοντας αποκλείσει δυνατότητες που εμφανίζονται στις προηγούμενες περιπτώσεις, έπεται ότι $j \equiv (k-j)\mathrm{mod}(p)$ και $k \equiv (i-k)\mathrm{mod}(p)$. Οπότε έπεται ότι $8j \equiv j\mathrm{mod}(p)$, δηλαδή πάλι $p = 7$ και η απόδειξη τελείωσε.

□

Θεώρημα 3.2.11. *Έστω $\overline{\mathcal{G}_{23}} \subseteq \mathcal{R}_{23}$ ένας δυαδικός κυκλικός κώδικας με γεννήτορα πολυώνυμο $\gamma(x) = x^{11} + x^{10} + x^6 + x^5 + x^4 + x^2 + 1$. Ο κώδικας $\overline{\mathcal{G}_{23}}$ είναι ένας τέλειος κώδικας με παραμέτρους* [23, 12, 7].

Απόδειξη. Από το Λήμμα 3.2.9 έχουμε ότι για κάθε (κωδικο)λέξη περιτού βάρους, έστω w, ισχύει $w^2 - w + 1 \geq 23$, δηλαδή $w \geq 7$. Από το Λήμμα 3.2.10 έχουμε ότι οι (κωδικο)λέξεις αρτίου βάρους έχουν βάρος μεγαλύτερο του 8. Αλλά η (κωδικο)λέξη $\gamma(x) = x^{11}+x^{10}+x^6+x^5+x^4+x^2+1$ έχει βάρος 7, άρα ο κώδικας έχει παραμέτρους [23, 12, 7]. Επιπλέον, επειδή ισχύει $2^{12}\left[1+23+\binom{23}{2}+\binom{23}{3}\right] = 2^{23}$, ο κώδικας είναι τέλειος. □

Παρατηρήσεις 3.2.12.

1. Ο κώδικας $\overline{\mathcal{G}_{23}}$ έχει τις ίδιες παραμέτρους με τον κώδικα Golay $\mathcal{G}_{23}$. Όπως θα δούμε στην επόμενη παράγραφο (Θεώρημα 3.3.4) οι δύο κώδικες είναι ισοδύναμοι, άρα ο κώδικας Golay $\mathcal{G}_{23}$ είναι κυκλικός.

2. Αξίζει να σημειωθεί ότι τα δύο προηγούμενα λήμματα ισχύουν γενικά για οποιονδήποτε περιττό πρώτο p και όχι συγκεκριμένα για τον $p = 23$.

3. Στην περίπτωση όπου $p = 7$ έχουμε ότι $x^7 - 1 = (x-1)(x^3+x+1)(x^3+x^2+1)$. Το πολυώνυμο x^3+x^2+1 είναι αμοιβαίο με το πολυώνυμο $x^3 + x + 1$ και ο κυκλικός κώδικας $\langle x^3 + x + 1\rangle$ περιέχει (κωδικο)λέξεις βάρους 4 (υπολογίστε μια τουλάχιστον (κωδιο)λέξη βάρους 4!). Άρα πράγματι η εξαίρεση του $p = 7$ στο Λήμμα 3.2.10 είναι αναγκαία.

4. Με τις υποθέσεις του Λήμματος 3.2.9, αν έχουμε εξασφαλίσει ότι η ελάχιστη απόσταση, έστω d, του κώδικα $\langle g_1(x)\rangle$ είναι περιττή, τότε ισχύει $d \geq \sqrt{p}$. Η τελευταία σχέση είναι γνωστή ως *φράγμα της τετραγωνικής ρίζας*.

   Υπάρχει μια ενδιαφέρουσα οικογένεια κωδίκων, οι κώδικες *τετργωνικών υπολοίπων*, στην οποία ανήκει και ο κωδικας Golay $\mathcal{G}_{23}$, όπου η ελάχιστη απόσταση πληροί το φράγμα της τετραγωνικής ρίζας. Εδώ δεν θα ασχοληθούμε με κώδικες τετραγωνικών υπολοίπων. Ο ενδιαφερόμενος αναγνώστης μπορεί να ανατρέξει στην παρατιθέμενη βιβλιογραφία για μια εισαγωγή σ΄ αυτούς τους κώδικες.

Τώρα θα εξετάσουμε την περίπτωση του τριαδικού κώδικα $\mathcal{G}_{11}$. Θεωρούμε δεδομένη την ανάλυση του πολυωνύμου $x^{11}-1$ σε γινόμενο αναγώγων πολυωνύμων επί του $\mathbb{Z}_3$. Δηλαδή $x^{11}-1 = (x-1)\cdot g_1(x)\cdot g_2(x)$, όπου $g_1(x) = x^5+x^4-x^3+x^2-1$ και $g_2(x) = x^5-x^3+x^2-x-1$. Παρατηρούμε ότι $g_2 = (-x^5)(g_1(x)$, επομένως οι κυκλικοί κώδικες $\langle g_1(x)\rangle$ και $\langle g_2(x)\rangle$ είναι ισοδύναμοι με παραμέτρους [11, 6, ?]. Θα υπολογίσουμε την ελάχιστη απόσταση του κώδικα $\mathcal{C} = \langle g_1(x)\rangle \subseteq \mathcal{R}_{11}$.

Έστω ο κυκλικός κώδικας $\mathcal{D} = \langle (x-1)g_1(x)\rangle$, προφανώς ο $\mathcal{D}$ περιέχεται στον κώδικα $\mathcal{C}$ και είναι διάστασης 5. Επίσης από το Θεώρημα 2.6.28 έχουμε ότι ο κώδικας $\mathcal{D}$ είναι μηδενικού αθροίσματος, δηλαδή αν
$d(x) = d_0 + d_1x + \cdots + d_{10}x^{10} \in \mathcal{D}$, τότε $\sum_{i=0}^{10} d_i = 0$.

Ο δυϊκός κώδικας $\mathcal{D}^\perp$ παράγεται από το αμοιβαίο πολυώνυμο του $g_2(x)$ (βλέπε Παρατήρηση 2.6.26) , δηλαδή το πολυώνυμο $-g_1(x)$. Αυτό σημαίνει ότι $\mathcal{D}^\perp = \langle -g_1(x)\rangle = \mathcal{C}$. Επομένως για το $d(x) = d_0 + d_1x + \cdots + d_{10}x^{10} \in \mathcal{D}$ έχουμε ότι είναι κάθετο στον εαυτό του. Δηλαδή $\sum_{i=0}^{10} d_i^2 \equiv 0 \mathrm{mod}(3)$.

Έστω w το βάρος του στοιχείου $d(x) = d_0 + d_1x + \cdots + d_{10}x^{10} \in \mathcal{D}$, το w παριστά τον αριθμό των μη μηδενικών συντελεστών d_i. Αλλά, επειδή $d_i \in \mathbb{Z}_3$, έχουμε ότι για $d_i \neq 0$ ισχύει $d_i^2 \equiv 1 \mathrm{mod}(3)$, οπότε $w \equiv \sum_{i=0}^{10} d_i^2 \mathrm{mod}(3)$.

Από τα προηγούμενα έπεται η επομένη πρόταση.

Πρόταση 3.2.13. *Έστω $\mathcal{D}$ και $\mathcal{C}$ όπως προηγουμένως, αν $d(x) = d_0 + d_1x + \cdots + d_{10}x^{10} \in \mathcal{D}$ με βάρος w, τότε $\sum_{i=0}^{10} d_i = 0$ και $w \equiv \sum_{i=0}^{10} d_i^2 \equiv 0 \mathrm{mod}(3)$.*

Επειδή η διάσταση του κώδικα $\mathcal{C}$ είναι 6 υπάρχουν τρία διαφορετικά σύμπλοκα του υπόχωρου $\mathcal{D}$ στο χώρο $\mathcal{C}$. Η (κωδικο)λέξη $a(x) = x^{10}+x^9+\cdots+x+1$ ανήκει στον κώδικα $\mathcal{C}$, αλλά δεν ανήκει στον $\mathcal{D}$, επομένως ο κώδικας $\mathcal{C}$ είναι η διακεκριμένη ένωση $\mathcal{C} = \mathcal{D} \cup (a(x)+\mathcal{D}) \cup (-a(x)+\mathcal{D})$.

Έστω $c(x) \in \mathcal{C}$ με $c(x) \notin \mathcal{D}$, χωρίς βλάβη, υποθέτουμε ότι $c(x) = d(x)+a(x)$ με $d(x) = d_0 + d_1x + \cdots + d_{10}x^{10} \in \mathcal{D}$, δηλαδή

$c(x) = (d_0+1)+(d_1+1)x+\cdots+(d_{10}+1)x^{10}$. Οπότε, όπως προηγουμένως $w(c(x)) \equiv \sum_{i=0}^{10}(d_i+1)^2 \mathrm{mod}(3)$. Από την τελευταία σχέση έχουμε ότι $w(c(x)) \equiv \big[\sum_{i=0}^{10} d_i^2 + 2\sum_{i=0}^{10} d_i + 11\big]\mathrm{mod}(3)$. Αλλά από την προηγούμενη πρόταση έχουμε ότι $\sum_{i=0}^{10} d_i^2 \equiv \sum_{i=0}^{10} d_i \equiv 0\mathrm{mod}(3)$. Οπότε
$w(c(x)) \equiv 11 \equiv 2\mathrm{mod}(3)$.

Από την τελευταία σχέση έπεται ότι το βάρος ενός $c(x) \in \mathcal{C}$ με $c(x) \notin \mathcal{D}$ είναι μεγαλύτερο ή ίσο του 5, εκτός εάν είναι ίσο με 2. Αλλά αν $w(c(x)) = 2$, τότε $c(x) = x^i + x^j$ με $0 \le i < j \le 10$, όμως το γινόμενο $c(x)\cdot c(x^{-1})$ πρέπει να είναι πολλαπλάσιο του $g_1(x)\cdot g_2(x) = x^{10}+x^9+\cdots+x+1$, άτοπο.

Ανακεφαλαιώνοντας έχουμε την επομένη πρόταση.

Πρόταση 3.2.14. *Έστω $\mathcal{D}$ και $\mathcal{C}$ όπως προηγουμένως, αν $c(x) \in \mathcal{C}$ με $c(x) \notin \mathcal{D}$, τότε $w(c(x)) \equiv 2\mathrm{mod}(3)$ και $w(c(x)) \ge 5$.*

Θεώρημα 3.2.15. *Ο κώδικας $\mathcal{C} = \langle g_1(x)\rangle$ είναι ένας $[11, 6, 5]$ τέλειος κώδικας.*

Απόδειξη. Ο κώδικας $\mathcal{C} = \langle g_1(x)\rangle$ έχει ελάχιστη απόσταση το πολύ 5, αφού έχει ένα στοιχείο, το $g_1(x) = x^5+x^4-x^3+x^2-1$, με βάρος ίσο με 5. Από την προηγούμενη πρόταση έχουμε ότι στοιχεία που δεν ανήκουν στον (υπο)κώδικα $\mathcal{D}$ έχουν βάρος μεγαλύτερο ή ίσον του 5. Επομένως αν η ελάχιστη απόσταση του κώδικα ήταν μικρότερη από 5, τότε θα έπρεπε να υπάρχει ένα στοιχείο $a(x) \in \mathcal{D}$ με βάρος μικρότερο ή ίσο του 4. Όμως από την Πρόταση 3.2.13 το βάρος του $a(x)$ είναι πολλαπλάσιο του 3. Υποθέτουμε ότι το στοιχείο $a(x) \in \mathcal{D}$ έχει βάρος 3. Χωρίς βλάβη της γενικότητας (επειδή ο κώδικας είναι κυκλικός μπορούμε να πάρουμε κυκλικές μεταθέσεις των στοιχείων του) υποθέτουμε ότι $a(x) = 1+x^i+x^j$ με τα i και j μή μηδενικά και διάφορα μεταξύ τους. Το $a(x)\cdot a(x^{-1})$ πρέπει να είναι πολλαπλάσιο του $(x-1)\cdot g_1(x)\cdot g_2(x) = x^{11}-1$, το οποίο είναι μηδέν στον $\mathcal{R}_{11}$. Δηλαδή έχουμε ότι $(1+x^i+x^j)\cdot(1+x^{-i}+x^{-j}) = x^i+x^{-i}+x^j+x^{-j}+x^{j-i}+x^{i-j} = 0$. Από την τελευταία σχέση έχουμε ότι $i \equiv j \equiv (j-i)\mathrm{mod}(11)$, δηλαδή $i \equiv 0\mathrm{mod}(11)$, άτοπο. Άρα τελικά η ελαχίστη απόσταση του κώδικα $\mathcal{C}$ ισούται με 5.

Επιπλέον ο κώδικας είναι τέλειος, αφού ισχύει $3^6\big[1+2\cdot 11+2^2\binom{11}{2}\big] = 3^{11}$. □

Ο κώδικας $\mathcal{C}$ έχει τις ίδιες παραμέτρους με τον κώδικα Golay $\mathcal{G}_{11}$. Όπως και στην περίπτωση του δυαδικού κώδικα Golay, ο κώδικας $\mathcal{C}$ είναι ισοδύναμος με τον τριαδικό κώδικα Golay $\mathcal{G}_{11}$. (Βλέπε Θεώρημα 3.3.4 .)

3.2.4 Ασκήσεις

1. Έστω A_i το πλήθος των στοιχείων βάρους i δε έναν κώδικα. Δείξτε ότι στον κώδικα $\mathcal{G}_{24}$ ισχύει $A_{20} = A_4 = 0$ $A_8 = A_{16} = ?$.

2. Δείξτε ότι αν $\mathbf{x}$ είναι μια δυαδική λέξη μήκους 23 και βάρους 4, τότε υπάρχει μοναδική (κωδικο)λέξη $\mathbf{c} \in \mathcal{G}_{23}$ βάρους 7 η οποία έχει 1 στις αντίστοιχες θέσεις που έχει 1 και η λέξη $\mathbf{x}$. Με τον τρόπο αυτό αποδείξτε ότι το πλήθος των κωδικολέξεων βάρους 7 στον κώδικα ισούται με 253.

3. Δείξτε ότι στον κώδικα $\mathcal{G}_{11}$ το πλήθος των στοιχείων βάρους 5 είναι ίσο με 132. (Υπόδειξη: Χρησιμοποιείστε το γεγονός ότι ο κώδικας $\mathcal{G}_{11}$ είναι τέλειος και υπολογίστε το πλήθος των ζευγών των λέξεων $(\mathbf{x}, \mathbf{c})$, όπου $\mathbf{x} \in \mathbb{Z}_2^{11}$ και έχει βάρος 3 και $\mathbf{c} \in \mathcal{G}_{11}$, έχει βάρος 5 και οι μη μηδενικές θέσεις της $\mathbf{x}$ συμπίπτουν με τις αντίστοιχες μη μηδενικές θέσεις της $\mathbf{c}$.)

4. Δείξτε ότι μεταθέτοντας στήλες και εφαρμόζοντας στοιχειώδεις πράξεις γραμμών ένας γεννήτορας πίνακας του κώδικα $\mathcal{G}_{24}$ μπορεί να λάβει τη μορφή $\begin{pmatrix} \mathrm{I}_7 & * \\ \mathbf{0}_5 & * \end{pmatrix}$, όπου η 8^η στήλη είναι το άθροισμα των επτά πρώτων στηλών.

5. Έστω H ένας πίνακας ελέγχου ισοτιμίας για τον κώδικα Hamming $\mathcal{H}(2, 3)$ και J ο τετραγωνικός πίνακας 4×4 με όλα τα στοιχεία του 1. Δείξτε ότι ο πίνακας $\mathrm{G} = \begin{pmatrix} \mathrm{J}+\mathrm{I}_4 & \mathrm{I}_4 & \mathrm{I}_4 \\ \mathbf{0} & \mathrm{H} & -\mathrm{H} \end{pmatrix}$ είναι ο γεννήτορας πίνακας ενός κώδικα ισοδυνάμου με τον κώδικα $\mathcal{G}_{12}$.

3.3 Η μοναδικότητα των κωδίκων Hamming και Goley ως τέλειοι κώδικες

Στην Παράγραφο 1.5 είχαμε αναφέρει (αλλά είχαμε αναβάλει την απόδειξη) ότι παρ'ολο που οι παράμετροι $(n, M, d) = (90, 2^{78}, 5)$ ικανοποιούν τη συνθήκη 1.5.2, δεν υπάρχουν κώδικες με αυτές τις παραμέτρους. Τώρα μπορούμε να δώσουμε μια απόδειξη.

Θεώρημα 3.3.1. *Δεν υπάρχει γραμμικός δυαδικός κώδικας με παραμέτρους* $[90, 78, 5]$.

Απόδειξη. Υποθέτουμε ότι υπάρχει ένας δυαδικός γραμμικός κώδικας με τις παραπάνω παραμέτρους. Έστω H ένας πίνακας ελέγχου ισοτιμίας αυτού του κώδικα. Ο πίνακας αυτός είναι ένας 12×90 πίνακας, ας συμβολίσουμε με $\mathbf{h}_1, \mathbf{h}_2, \ldots, \mathbf{h}_{90}$ τις στήλες του. Από την Πρόταση 2.2.27 έπεται ότι κάθε τετράδα από τις στήλες $\mathbf{h}_i$ είναι γραμμικά ανεξάρτητες. Επομένως το σύνολο $\mathrm{A} = \{\, \mathbf{0}, \mathbf{h}_i, \mathbf{h}_j+\mathbf{h}_k \mid 1 \le i \le 90, 1 \le j < k \le 90 \,\}$ περιέχει $1+90+\binom{90}{2} = 2^{12}$ το πλήθος στοιχεία. Αν οι στήλες του πίνακα H θεωρηθούν ως διανύσματα, βλέπουμε ότι το σύνολο A είναι το $\mathbb{Z}_2^{12}$. Ως γνωστόν (βλέπε Άσκηση $2.1.2_2$) το ήμισυ

των στοιχείων του $\mathbb{Z}_2^{12}$ έχουν περιττό βάρος, επομένως το σύνολο A περιέχει 2^{11} το πλήθος στοιχεία περιττού βάρους.

Ας υπολογίσουμε το πλήθος των στοιχείων του συνόλου A περιττού βάρους με διαφορετικό τρόπο. Υποθέτουμε ότι r το πλήθος από τις στήλες του πίνακα H έχουν περιττό βάρος, άρα οι αρτίου βάρους στήλες είναι $90-r$ το πλήθος. Από τη σχέση $w(\mathbf{h}_j+\mathbf{h}_k) = w(\mathbf{h}_j)+w(\mathbf{h}_k)-2w(\mathbf{h}_j\cap\mathbf{h}_k)$ (βλέπε 1.2.10) έχουμε ότι το βάρος του στοιχείου $\mathbf{h}_j+\mathbf{h}_k$ είναι περιττό αν και μόνο αν ακριβώς ένα από τα στοιχεία $\mathbf{h}_j$ και $\mathbf{h}_k$ είναι περιττού βάρους. Άρα το σύνολο A έχει $r+r(90-r)$ το πλήθος στοιχεία περιττού βάρους. Τελικά πρέπει να ισχύει $r+r(90-r) = 2^{11}$. Όπως εύκολα διαπιστώνουμε δεν υπάρχει θετικός ακέραιος που να πληροί την τελευταία σχέση. Άρα δεν υπάρχει γραμμικός δυαδικός κώδικας με παραμέτρους [90, 78, 5].

□

Το προηγούμενο θεώρημα αναφέρεται στην μη ύπαρξη γραμμικών κωδίκων με τις παραμέτρους $(n, M, d) = (90, 2^{78}, 5)$. Μπορούμε να αποδείξουμε ένα αποτέλεσμα που αναφέρεται στην μη ύπαρξη μη γραμμικών $(90, 2^{78}, 5)$ κωδίκων.

Ορισμός 3.3.2. *Έστω* $\mathbf{u}, \mathbf{v} \in \mathbb{Z}_2^n$, *το διάνυσμα* **u καλύπτει** *το* **v** *αν και μόνο αν* $\mathbf{u}\cap\mathbf{v} = \mathbf{v}$. *Δηλαδή στις θέσεις που το* **v** *έχει 1, έχει 1 οπωσδήποτε και το* **u**.

Για παράδειγμα το $\mathbf{u} = 110101$ καλύπτει το $\mathbf{v} = 010001$.

Πρόταση 3.3.3. *Δεν υπάρχει* $(90, 2^{78}, 5)$ *δυαδικός κώδικας.*

Απόδειξη. Υποθέτουμε ότι υπάρχει ένας $(90, 2^{78}, 5)$ κώδικας $\mathcal{C}$. Από την Πρόταση 1.4.4 έπεται ότι μπορούμε να υποθέσουμε ότι η μηδενική λέξη είναι στοιχείο του κώδικα ($\mathbf{0} \in \mathcal{C}$). Επειδή η ελάχιστη απόσταση είναι ίση με 5, κάθε μη μηδενική (κωδιο)λέξη έχει βάρος τουλάχιστον 5. Έστω Y το υποσύνολο του $\mathbb{Z}_2^{90}$, τα στοιχεία του οποίου έχουν βάρος 3 και τα δύο πρώτα ψηφία τους είναι 1, (δηλαδή μόνο τρία ψηφία τους είναι 1 εκ των οποίων τα δύο καταλαμβάνουν τις δύο πρώτες θέσεις και το τρίτο μια από τις υπόλοιπες 88) επομένως προφανώς $|Y| = 88$.

Ο κώδικας $\mathcal{C}$ είναι τέλειος, επομένως κάθε στοιχείο, έστω $\mathbf{y}$, του Y βρίσκεται σε μια μοναδική σφαίρα $S(\mathbf{x}, 2)$ ακτίνας ίσης με 2. Το κέντρο $\mathbf{x}$ της σφαίρας πρέπει να έχει βάρος ίσο με 5 και να καλύπτει το $\mathbf{y}$ (γιατί;).

Έστω X το σύνολο όλων των (κωδικο)λέξεων του $\mathcal{C}$, οι οποίες έχουν στις δύο πρώτες θέσεις 1 και το βάρος τους ισούται με 5. Κάθε στοιχείο $\mathbf{x}$ του συνόλου X καλύπτει ακριβώς τρία στοιχεία του σύνόλου Y. Πράγματι ένα στοιχείο $\mathbf{x}$ του X έχει δύο 1 στις δύο πρώτες θέσεις και τρία 1 τα οποία κατανέμονται στις υπόλοιπες 88 θέσεις, επομένως καλύπτει τα τρία στοιχεία του Y που το καθένα έχει (το τρίτο) 1 σε μια από τις τρείς θέσεις (εκτός της πρώτης και δεύτερης) που καταλαμβάνουν τα 1 του $\mathbf{x}$. Επομένως για ένα $\mathbf{x} \in X$ έχουμε τρία διαφορετικά

ζεύγη $(\mathbf{x}, \mathbf{y}_i)$, $i = 1, 2, 3$ με $\mathbf{y}_i \in Y$ έτσι ώστε $\mathbf{x}$ να καλύπτει το $\mathbf{y}_i$. Άρα αν $R = \{ (\mathbf{x}, \mathbf{y}) \,|\, \mathbf{x} \in X, \mathbf{y} \in Y \text{ και } \mathbf{x} \text{ καλύπτει το } \mathbf{y} \}$, τότε $| R | = 3 | X |$.
Αλλά ο κώδικας είναι τέλειος, επομένως δεν υπάρχουν δύο διαφορετικά $\mathbf{x}_1, \mathbf{x}_2 \in X$ που να καλύπτουν το ίδιο $\mathbf{y} \in Y$. Επομένως $| R | = | Y | = 88$.

Από τα προηγούμενα έπεται ότι $| X | = \frac{88}{3}$, άτοπο, άρα δεν υπάρχει $(90, 2^{78}, 5)$ δυαδικός κώδικας. □

Ανακεφαλαιώνοντας βλέπουμε ότι, πέραν των τετριμμένων, τέλειοι κώδικες είναι οι κώδικες Hamming $\mathcal{H}(r, p)$, και οι κώδικες Golay $\mathcal{G}_{23}$ και $\mathcal{G}_{11}$. Οι κώδικες αυτοί είναι γραμμικοί, στην Παρατήρηση $3.1.4_4$ είχαμε δει ότι υπάρχουν δυαδικοί κώδικες με τις παραμέτρους ενός κώδικα Hamming, οι οποίοι δεν είναι γραμμικοί. Έχουν κατασκευασθεί κώδικες επί ενός αλφαβητού $\mathbb{F}_p$, όπου $\mathbb{F}_p$ είναι ένα τυχαίο πεπερασμένο σώμα, με τις παραμέτρους ενός κώδικα Hamming, οι οποίοι δεν είναι γραμμικοί.

Στην πραγματικότητα δεν υπάρχουν άλλοι τέλειοι κώδικες επί ενός αλφαβητού $\mathbb{F}_p$, όπου $\mathbb{F}_p$ είναι ένα πεπερασμένο σώμα. Συγκεκριμένα ισχύει το εξής Θεώρημα:

Θεώρημα 3.3.4. *Ένας μη τετριμμένος τέλειος κώδικας επί ενός αλφαβητού $\mathbb{F}_p$ πρέπει να έχει είτε τις παραμέτρους ένος κώδικα Hamming ή τις παραμέτρους ενός από τους κώδικες Golay $\mathcal{G}_{23}$, $\mathcal{G}_{11}$.*

Επιπλέον, αν ένας κώδικας έχει τις παραμέτρους ενός από τους κώδικες Golay, τότε είναι ισοδύναμος προς αυτόν. Αν ένας κώδικας έχει τις παραμέτρους ενός από τους κώδικες Hamming και είναι γραμμικός, τότε είναι ισοδύναμος προς αυτόν.

Η απόδειξη αυτού του θεωρήματος είναι πέραν του σκοπού του παρόντος. Ο ενδιαφερόμενος μπορεί να βρεί μια κομψή απόδειξη στο MacWilliams-Sloane (1977). Αξίζει όμως να αναφέρουμε την κεντρική ιδέα, η οποία βασίζεται στο εξής θεώρημα του Lloyd, το οποίο παραθέτουμε και αυτό χωρίς απόδειξη.

Θεώρημα 3.3.5. *Εάν υπάρχει ένας τέλειος $(n, M, 2\lambda + 1)$ κώδικας επί του σώματος $\mathbb{F}_p$, όπου η τάξη του είναι ίση με q, τότε το πολυώνυμο*
$L(x) = \sum_{i=0}^{\lambda} (-1)^i (q-1)^{\lambda - i} \binom{x-1}{i} \binom{n-x}{\lambda - i}$ *έχει λ διακεκριμένες ακέραιες ρίζες μεταξύ του 1 και του n.*

Από το Θεώρημα αυτό αποδεικνύεται ότι αν υπάρχει ένας τέλειος κώδικας επί του $\mathbb{F}_p$, τότε πρέπει να ισχύει $\lambda \leq 11$, $q \leq 8$ και $n < 485$. Με την βοήθεια υπολογιστού στην αρχή και κατόπιν θεωρητικά απεδείχθει ότι αν υπάρχουν κώδικες των οποίων οι παράμετροι ικανοποιούν τα ανωτέρω φράγματα και οι οποίοι είναι τέλειοι, δηλαδή ισχύει η Πρόταση 1.5.12, είναι μόνο οι τετριμμένοι, οι κώδικες με παραμέτρους ίδιες με τις παραμέτρους των κωδίκων Hamming και Golay καθώς και κώδικες με παρμέτρους $(90, 2^{78}, 5)$ για τις οποίες έχουμε ήδη αποδείξει ότι δεν υπάρχουν κώδικες με αυτές τις παραμέτρους.

Εδώ μπορούμε να παρατηρήσουμε ότι η μη ύπαρξη τέλειων κωδίκων με παραμέτρους $(90, 2^{78}, 5)$ απορρέει και από το προηγούμενο θεώρημα, καθ' ότι για $\lambda = 2$ και $n = 90$ $L(x) = 0$ αν και μόνο αν $x^2 - 91x + 2048 = 0$ η τελευταία όμως εξίσωση δεν έχει ακέραιες λύσεις.

Το Θεώρημα 3.3.4 δίνει μια απάντηση ως προς τους τέλειους κώδικες, αλλά αφίνει πολλά ερωτηματικά.

Από τον τρόπο κατασκευής των κωδίκων Hamming (βλέπε Παρατήρηση 3.1.4) ένας γραμμικός κώδικας επί ενός πεπερασμένου σώματος $\mathbb{F}_p$ με τις παραμέτρους ενός κώδικα Hamming είναι ισοδύναμος με τον αντίστοιχο κώδικα Hamming. Αλλά αν ο κώδικας δεν είναι γραμμικός, τότε παραμένει το εξής πρόβλημα:

Να βρεθούν όλοι οι (μη ισοδύναμοι) μη γραμμικοί κώδικες, οι οποίοι έχουν τις παραμέτρους ενός κώδικα Hamming.

Το πρόβλημα παραμένει ανοικτό. Για παράδειγμα πιστεύεται ότι υπάρχουν πάρα πολλοί δυϊκοί κώδικες με παραμέτρους $(15, 2^{11}, 3)$.

Από την άλλη πλευρά έχει αποδειχθεί (όπως αναφέρεται και στο Θεώρημα 3.3.4) ότι κάθε κώδικας με τις παραμέτρους ενός από τους κώδικες Golay, τότε είναι ισοδύναμος προς έναν από αυτούς.

Ένα άλλο μεγάλο πρόβλημα, το οποίο και αυτό παραμένει ανοικτό, είναι το εξής:

Υπάρχουν τέλειοι κώδικες επί ενός αλφαβήτου του οποίου το πλήθος των στοιχείων δεν είναι δύναμη ενός πρώτου αριθμού;

Σχετικά με το τελευταίο πρόβλημα έχει αποδειχθεί ότι για $\lambda \geq 3$ ο μόνος μη τετριμμένος τέλειος κώδικας που διορθώνει λ το πλήθος λάθη είναι ο δυαδικός κώδικας Golay. Αλλά οι περιπτώσεις $\lambda = 2$ ή $\lambda = 1$ παραμένουν αναπάντητες.

Εδώ αξίζει να αναφέρουμε ένα μερικό αποτέλεσμα. Δεν υπάρχει $6-$αδικός $(7, 6^5, 3)$ κώδικας.
Ενδιαφέρον παρουσιάζει μια απόδειξη όπου η ύπαρξη $6-$αδικού $(7, 6^5, 3)$ κώδικα ανάγεται στην επίλυση του γνωστού προβλήματος του Euler των "36 αξιωματικών". Όπως όμως είναι γνωστόν [1] το πρόβλημα αυτό έχει αρνητική απάντηση, επομένως δεν υπάρχει $6-$αδικός $(7, 6^5, 3)$ κώδικας.

[1] Για περισσότερες πληροφορίες ως προς αυτό το πρόβλημα, όπως και γενικότερα για τα Λατινικά τετράγωνα, ο ενδιαφερόμενος αναγνώστης μπορεί να ανατρέξει σε ένα εγχειρίδιο Συνδυαστικής.

3.4 Κώδικες Reed-Muller

Οι κώδικες Reed-Muller είναι από τις πρώτες οικογένειες κωδίκων, οι οποίοι, αν και δεν είναι τόσο αποτελεσματικοί, έχουν χρησιμοποιηθεί εκτενώς, διότι έχουν το πλεονέκτημα της εύκολης αποκωδικοποίησης. Όπως έχουμε ήδη αναφέρει (βλέπε σελ. 12) οι κώδικες Reed-Muller έχουν χρησιμοποιηθεί για την αποστολή ασπρόμαυρων φωτογραφιών από τον πλανήτη Άρη.

Υπάρχουν πολλοί τρόποι για να ορίσουμε τους κώδικες Reed-Muller. Εδώ θα παρουσιάσουμε έναν επαγωγικό τρόπο ορισμού των.

Ορισμός 3.4.1. *Για κάθε ακέραιο αριθμό $m \geq 1$ ορίζουμε τους κώδικες Reed-Muller πρώτης τάξης και συμβολίζουμε $\mathcal{RM}_1(m) =: \mathcal{RM}(m)$ ως εξής:*
Για $m = 1$ $\mathcal{RM}(1) = \mathbb{Z}_2^2 = \{\, 00,\, 01,\, 10,\, 11 \,\}$.
Για $m \geq 1$ $\mathcal{RM}(m+1) = \mathcal{RM}(m) \oplus \mathcal{R}_2(2^m) = \{\, \mathbf{u}(\mathbf{u}+\mathbf{v}) \mid \mathbf{u} \in \mathcal{RM}(m),\, \mathbf{v} \in \mathcal{R}_2(2^m) \,\}$, *όπου $\mathcal{R}_2(2^m)$ είναι ο επαναληπτικός δυαδικός κώδικας* $\{\, \underbrace{00\cdots0}_{2^m-\text{φορές}},\, \underbrace{11\cdots1}_{2^m-\text{φορές}} \,\}$.

(Για την $(\mathbf{u},\, \mathbf{u}+\mathbf{v})$-κατασκευή του κώδικα $\mathcal{RM}(m) \oplus \mathcal{R}_2(2^m)$ βλέπε σελ. 41.)

Παράδειγμα 3.4.2. Εφαρμόζοντας τον ορισμό εύκολα μπορούμε να κατασκευάσουμε τον κώδικα $\mathcal{RM}(2) = \{\, 0000,\, 0011,\, 0101,\, 0110,\, 1010,\, 1001,\, 1111,\, 1100 \,\}$.

Θεώρημα 3.4.3. *Για κάθε $m \geq 1$ ο κώδικας $\mathcal{RM}(m)$ είναι γραμμικός με παραμέτρους $[2^m,\, m+1,\, 2^{m-1}]$. Επίσης κάθε (κωδικο)λέξη, εκτός της $\mathbf{0}$ και $\mathbf{1}$, έχει βάρος ίσο με 2^{m-1}.*

Απόδειξη. Προφανώς ο κώδικας $\mathcal{RM}(1)$ είναι γραμμικός. Υποθέτοντας ότι ο $\mathcal{RM}(m)$ είναι γραμμικός αποδεικνύεται εύκολα ότι και ο $\mathcal{RM}(m+1)$ είναι γραμμικός. Επίσης από τον ορισμό έπεται ότι το μήκος κάθε (κωδικο)λέξης του $\mathcal{RM}(m+1)$ είναι διπλάσιο από το μήκος κάθε (κωδικο)λέξης του $\mathcal{RM}(m)$, οπότε με επαγωγή έπεται ότι το μήκος του $\mathcal{RM}(m)$ είναι ίσο με 2^m.

Ο κώδικας $\mathcal{RM}(m+1)$ αποτελείται από δύο κατηγορίες στοιχείων. Τα στοιχεία της μορφής $\mathbf{uu}$ με $\mathbf{u} \in \mathcal{RM}(m)$ και τα στοιχεία της μορφής $\mathbf{u}(\mathbf{u}+\mathbf{1})$ με $\mathbf{u} \in \mathcal{RM}(m)$ και $\mathbf{1} = \underbrace{11\cdots1}_{2^m-\text{φορές}}$. Κάθε κατηγορία περιλαμβάνει $|\mathcal{RM}(m)|$ το πλήθος στοιχεία και δεν υπάρχει στοιχείο που να ανήκει και στις δύο κατηγορίες, επομένως $|\mathcal{RM}(m+1)| = 2 \cdot |\mathcal{RM}(m)| = 2 \cdot 2^{m+1}$.

Έστω τώρα ένα στοιχείο $\mathbf{c} \in \mathcal{RM}(m+1)$, το οποίο είναι διάφορο των $\mathbf{0}$ και $\mathbf{1}$. Αν είναι της μορφής $\mathbf{uu}$ με $\mathbf{u} \in \mathcal{RM}(m)$, τότε το $\mathbf{u}$ είναι διάφορο των $\mathbf{0}$ και $\mathbf{1}$ και συνεπώς, υποθέτοντας ότι το βάρος του $\mathbf{u}$ είναι ίσο με 2^{m-1}, έχουμε

$w(\mathbf{c}) = 2w(\mathbf{u}) = 2 \cdot 2^{m-1} = 2^m$. Έστω ότι το $\mathbf{c}$ είναι της μορφής $\mathbf{u}(\mathbf{u}+\mathbf{1})$ με $\mathbf{u} \in \mathcal{RM}(m)$. Στην περίπτωση που $\mathbf{u} = \mathbf{0}$ ή $\mathbf{u} = \mathbf{1}$, προφανώς το βάρος του $\mathbf{c} = \mathbf{u}(\mathbf{u}+\mathbf{1})$ είναι ίσο με 2^m. Υποθέτουμε ότι το $\mathbf{u}$ είναι διάφορο των $\mathbf{0}$ και $\mathbf{1}$, τότε $w(\mathbf{c}) = w(\mathbf{u}) + w(\mathbf{u}+\mathbf{1}) = w(\mathbf{u}) + w(\mathbf{u}) + w(\mathbf{1}) - 2w(\mathbf{u} \cap \mathbf{1})$ (βλέπε Πρόταση 1.2.10). Αλλά $\mathbf{u} \cap \mathbf{1} = \mathbf{u}$, οπότε από την προηγούμενη σχέση έχουμε $w(\mathbf{c}) = w(\mathbf{u}) + w(\mathbf{u}) + w(\mathbf{1}) - 2w(\mathbf{u}) = w(\mathbf{1}) = 2^m$. Επομένως σε όλες τις περιπτώσεις έχουμε $w(\mathbf{c}) = 2^m$ και η απόδειξη τελείωσε.

□

Επαγωγικά μπορούμε να υπολογίσουμε τους γεννήτορες πίνακες των κωδίκων $\mathcal{RM}(m)$ για $m \geq 1$.

Θεώρημα 3.4.4. *Ένας γεννήτορας πίνακας του κώδικα $\mathcal{RM}(1)$ είναι ο πίνακας* $\mathrm{R}_1 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$.

Αν R_m είναι ένας γεννήτορας πίνακας του κώδικα $\mathcal{RM}(m)$, τότε ο πίνακας $\mathrm{R}_{m+1} = \left(\begin{array}{ccc|ccc} 0 & \cdots & 0 & 1 & \cdots & 1 \\ \hline \multicolumn{3}{c|}{\mathrm{R}_m} & \multicolumn{3}{c}{\mathrm{R}_m} \end{array}\right)$ *είναι γεννήτορας πίνακας του $\mathcal{RM}(m+1)$.*

Απόδειξη. Προφανώς ο πίνακας R_1 είναι ένας γεννήτορας πίνακας του κώδικα $\mathcal{RM}(1)$.

Υποθέτουμε ότι ο πίνακας R_m είναι ένας γεννήτορας πίνακας του κώδικα $\mathcal{RM}(m)$, τότε $\mathcal{RM}(m) = \{\, \mathbf{r} \cdot \mathrm{R}_m \mid \mathbf{r} \in \mathbb{Z}_2^{m+1} \,\}$.

Έστω ένα στοιχείο $\mathbf{u} \in \mathcal{RM}(m)$, τότε υπάρχει $\mathbf{r} \in \mathbb{Z}_2^{m+1}$ έτσι ώστε $\mathbf{u} = \mathbf{r} \cdot \mathrm{R}_m$, επισυνάπτοντας στην αρχή του $\mathbf{r}$ την συντεταγμένη 0, το στοιχείο $0\,\mathbf{r}$ ανήκει στο $\mathbb{Z}_2^{m+2}$ και για το στοιχείο $\mathbf{uu} \in \mathcal{RM}(m+1)$ έχουμε ότι $\mathbf{uu} = (0\,\mathbf{r}) \cdot \left(\begin{array}{ccc|ccc} 0 & \cdots & 0 & 1 & \cdots & 1 \\ \hline \multicolumn{3}{c|}{\mathrm{R}_m} & \multicolumn{3}{c}{\mathrm{R}_m} \end{array}\right)$. Επισυνάπτοντας στην αρχή του $\mathbf{r}$ την συντεταγμένη 1, το στοιχείο $1\,\mathbf{r}$ ανήκει στο $\mathbb{Z}_2^{m+2}$ και για το στοιχείο $\mathbf{u}(\mathbf{u}+\mathbf{1}) \in \mathcal{RM}(m+1)$ έχουμε ότι $\mathbf{u}(\mathbf{u}+\mathbf{1}) = (1\,\mathbf{r}) \cdot \left(\begin{array}{ccc|ccc} 0 & \cdots & 0 & 1 & \cdots & 1 \\ \hline \multicolumn{3}{c|}{\mathrm{R}_m} & \multicolumn{3}{c}{\mathrm{R}_m} \end{array}\right)$.

Από τα προηγούμενα έπεται ότι $\mathcal{RM}(m+1) \subseteq \{\, \mathbf{c} \cdot \mathrm{R}_{m+1} \mid \mathbf{c} \in \mathbb{Z}_2^{m+2} \,\}$.

Η τάξη του πίνακα R_{m+1} είναι το πολύ ίση με $m+2$, επομένως ο χώρος $\{\, \mathbf{c} \cdot \mathrm{R}_{m+1} \mid \mathbf{c} \in \mathbb{Z}_2^{m+2} \,\}$ έχει διάσταση το πολύ ίση με $m+2$, οπότε από την προηγούμενη σχέση έχουμε ότι, (αφού η διάσταση του $\mathcal{RM}(m+1)$ είναι ίση με $m+2$,) $\mathcal{RM}(m+1) = \{\, \mathbf{c} \cdot \mathrm{R}_{m+1} \mid \mathbf{c} \in \mathbb{Z}_2^{m+2} \,\}$ και ο πίνακας R_{m+1} είναι γεννήτορας πίνακας του $\mathcal{RM}(m+1)$.

(Επειδή κάθε στοιχείο $\mathbf{c} \in \mathbb{Z}_2^{m+2}$ είναι της μορφής $0\,\mathbf{r}$ ή $1\,\mathbf{r}$ με $\mathbf{r} \in \mathbb{Z}_2^{m+1}$, έχουμε ότι και $\{\, \mathbf{c} \cdot \mathrm{R}_{m+1} \mid \mathbf{c} \in \mathbb{Z}_2^{m+2} \,\} \subseteq \mathcal{RM}(m+1)$).

□

Παράδειγμα 3.4.5. Έχοντας ότι ο πίνακας $\mathrm{R}_1 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$ είναι γεννήτορας πίνακας του κώδικα $\mathcal{RM}(1)$, οι πίνακες $\mathrm{R}_2 = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix}$ και $\mathrm{R}_3 = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$ είναι γεννήτορες πίνακες των κωδίκων $\mathcal{RM}(2)$ και $\mathcal{RM}(3)$ αντίστοιχα.

Από τον προηγούμενο επαγωγικό τρόπο κατασκευής των γεννητόρων πινάκων των κωδίκων $\mathcal{RM}(m)$ μπορούμε να συνάγουμε έναν απ΄ ευθείας τρόπο υπολογισμού των.

Πρόταση 3.4.6. 1) *Η πρώτη γραμμή του πίνακα* R_m *αποτελείται από ένα τμήμα με* 2^{m-1} *το πλήθος 0 και από ένα τμήμα με* 2^{m-1} *το πλήθος 1, δηλαδή είναι της μορφής* $\underbrace{00\cdots0}_{2^{m-1}}\underbrace{11\cdots1}_{2^{m-1}}$. *Η δεύτερη γραμμή αποτελείται από δύο τμήματα με* 2^{m-2} *το πλήθος 0 και από δύο τμήματα με* 2^{m-2} *το πλήθος 1, τα οποία εναλλάσονται μεταξύ τους, δηλαδή είναι της μορφής*

$\underbrace{00\cdots0}_{2^{m-2}}\underbrace{11\cdots1}_{2^{m-2}}\underbrace{00\cdots0}_{2^{m-2}}\underbrace{11\cdots1}_{2^{m-2}}$.

Γενικά η i *γραμμή αποτελείται από τμήματα που αποτελούνται από 0 και από τμήματα που αποτελούνται από 1 μήκους* 2^{m-i}, *τα οποία εναλλάσονται μεταξύ τους. Οπότε η προτελευταία γραμμή αποτελείται απο εναλλασόμενα 0 και 1. Απομένει η τελευταία γραμμή, της οποίας όλα τα στοιχεία είναι 1.*

2) *Οι στήλες του* R_m *μπορούν να περιγραφούν ως εξής: Αν εξαιρέσουμε το τελευταίο στοιχείο κάθε στήλης, το οποίο είναι πάντα 1, τότε τα τμήματα που απομένουν αναπαριστούν (διαβάζοντας από άνω προς τα κάτω) κατά σειρά τους αριθμούς* $0, 1, \ldots, 2m-1$ *σε δυαδική μορφή.*

Απόδειξη. Η απόδειξη συνίσταται σε απλή παρατήρηση του πίνακα $\mathrm{R}_{m+1} = \left(\begin{array}{ccc|ccc} 0 & \cdots & 0 & 1 & \cdots & 1 \\ \hline \multicolumn{3}{c|}{\mathrm{R}_m} & \multicolumn{3}{c}{\mathrm{R}_m} \end{array}\right)$.

□

3.4.1 Σύγκριση των κωδίκων Hamming και Reed-Muller

Έστω ότι έχουμε τον δυαδικό κώδικα Hamming $\mathcal{H}(m, 2)$ με παραμέτρους $[n = 2^m - 1), k = 2^m - 1 - m, 3]$ και τον κώδικα Reed-Muller $\mathcal{RM}(m)$ με

παραμέτρους $[2^m,\, m+1,\, 2^{m-1}]$. Ο δυϊκός κώδικας $\mathcal{H}(m,\,2)^{\perp}$ έχει παραμέτρους $[n\,=\,2^m-1),\, m,\, 2^{m-1}]$. Όπως βλέπουμε, αν θέλουμε να συγκρίνουμε δύο κώδικες προτιμιταίο είναι να συγκρίνουμε τον κώδικα $\mathcal{S}(m)\,=:\mathcal{H}(m,\,2)^{\perp}$ με τον κώδικα $\mathcal{RM}(m)$ που έχουν *παρεμφερείς* παραμέτρους.

Επεκτείνουμε τον κώδικα Hamming $\mathcal{H}(m,\,2)$ επισυνάπτοντας στην αρχή κάθε στοιχείου του ένα ψηφίο ελέγχου ισοτιμίας. [2] Την επέκταση που προκύπτει τη συμβολίζουμε με $\mathcal{EH}(m,\,2)$. Ο πίνακας Hamming H_m είναι πίνακας ελέγχου ισοτιμίας του κώδικα $\mathcal{H}(m,\,2)$, επομένως για κάθε $\mathbf{c}\in\mathcal{H}(m,\,2)$ ισχύει $\mathbf{c}\mathrm{H}_m^t\,=\,\mathbf{0}$. Δεν είναι δύσκολο να δούμε ότι ένας πίνακας ελέγχου ισοτιμίας του κώδικα $\mathcal{EH}(m,\,2)$ είναι ο πίνακας $\mathrm{EH}_m\,=\,\left(\begin{array}{c|ccc} 0 & & & \\ \vdots & & \mathrm{H}_m & \\ 0 & & & \\ \hline & & & \\ 1 & 1 & \cdots & 1 \end{array}\right)$.

Δηλαδή ο πίνακας EH_m προέρχεται από τον πίνακα H_m αν επισυνάψουμε μια πρώτη στήλη που αποτελείται από 0 και κατόπιν επισυνάψουμε μια τελευταία γραμμή που αποτελείται από 1.

Από τα δύο πρώτα Παραδείγματα 3.1.2 έχουμε ότι οι πίνακες ελέγχου ισοτιμίας για τους κώδικες $\mathcal{EH}(2,\,2)$ και $\mathcal{EH}(3,\,2)$ αντίστοιχα είναι οι πίνακες $\mathrm{EH}_2\,=\,\left(\begin{array}{cccc} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 \end{array}\right)$ και $\mathrm{EH}_3\,=\,\left(\begin{array}{cccccccc} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{array}\right)$.

Παρατηρούμε ότι $\mathrm{EH}_3\,=\,\left(\begin{array}{ccc|ccc} 0 & \cdots & 0 & 1 & \cdots & 1 \\ \hline & \mathrm{EH}_2 & & & \mathrm{EH}_2 & \end{array}\right)$.

Η παρατήρηση αυτή ιχύει γενικά για κάθε $m\geq 2$. Πράγματι, από την Πρόταση 3.1.5 έχουμε έναν αναγωγικό τρόπο υπολογισμού του πίνακα H_{m+1}, δηλαδή $\mathrm{H}_{m+1}\,=\,\left(\begin{array}{ccc|c|ccc} 0 & \cdots & 0 & 1 & 1 & \cdots & 1 \\ \hline & & & 0 & & & \\ & \mathrm{H}_m & & \vdots & & \mathrm{H}_m & \\ & & & 0 & & & \end{array}\right)$.

Αν τον *συνδυάσουμε* με τον πίνακα $\mathrm{EH}_m\,=\,\left(\begin{array}{c|ccc} 0 & & & \\ \vdots & & \mathrm{H}_m & \\ 0 & & & \\ \hline & & & \\ 1 & 1 & \cdots & 1 \end{array}\right)$, έχουμε

[2] Συνήθως το ψηφίο ελέγχου ισοτιμίας επισυνάπτεται στο τέλος κάθε (κωδικο)λέξης (βλέπε σελ. 36), εδώ το επισυνάπτομε στην αρχή.

ότι $\mathrm{EH}_{m+1} = \left(\begin{array}{ccc|ccc} 0 & \cdots & 0 & 1 & \cdots & 1 \\ \hline & \mathrm{EH}_m & & & \mathrm{EH}_m & \end{array}\right)$.

Στο Παράδειγμα 3.4.5 είχαμε υπολογίσει τους γεννήτορες πίνακες $\mathrm{R}_2 = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix}$ και $\mathrm{R}_3 = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$ των κωδίκων $\mathcal{RM}(2)$ και $\mathcal{RM}(3)$ αντίστοιχα. Όπως βλέπουμε $\mathrm{R}_2 = \mathrm{EH}_2$ και $\mathrm{R}_3 = \mathrm{EH}_3$. Από το Θεώρημα 3.4.4 και τα προηγούμενα βλέπουμε ότι για κάθε $m \geq 1$ έχουμε ότι $\mathrm{R}_m = \mathrm{EH}_m$.

Πρόταση 3.4.7. *Ο κώδικας Reed-Muller $\mathcal{RM}(m)$ είναι ίσος με τον δυϊκό κώδικα του επεκταμένου δυαδικού κώδικα Hamming $\mathcal{EH}(m, 2)$.*

Απόδειξη. Οι δύο κώδικες είναι γραμμικοί και έχουν τον ίδιο γεννήτορα πίνακα. □

Παρατήρηση 3.4.8. Έχοντας τον κώδικα Reed-Muller $\mathcal{RM}(m)$ εφαρμόζουμε την αντίστροφη διαδικασία. Δηλαδή πέρνουμε μόνο τις (κωδικο)λέξεις που αρχίζουν από 0 και κατόπιν διαγράφουμε το 0 από την πρώτη θέση. Ο κώδικας που προκύπτει από αυτή τη συμπύκνωση δεν είναι παρά ο δυϊκός κώδικας $\mathcal{S}(m) = \mathcal{H}(m, 2)^{\perp}$.

3.4.2 Κώδικες Reed-Muller ανώτερης τάξης

Έχοντας ορίσει τους κώδικες Reed-Muller $\mathcal{RM}_1(m) = \mathcal{RM}(m)$ πρώτης τάξης για $m \geq 1$, μπορούμε για $2 \leq r \leq m$ να ορίσουμε τους κώδικες Reed-Muller $r-$τάξης ως εξής: $\mathcal{RM}_r(r) = \mathbb{Z}_2^{2^r}$ και $\mathcal{RM}_r(m+1) = \mathcal{RM}_r(m) \oplus \mathcal{RM}_{r-1}(m)$, όπου $\oplus$ παριστά την $(\mathbf{u}, \mathbf{u}+\mathbf{v})$- κατασκευή.

Επαγωγικά μπορούμε να αποδείξουμε (η απόδειξη αφίνεται ως άσκηση), επικαλούμενοι και την Πρόταση 1.4.12, ότι οι κώδικες $\mathcal{RM}_r(m)$ είναι γραμμικοί με παραμέτρους $[2^m, k, 2^{m-r}]$, όπου $k = 1 + \binom{m}{1} + \binom{m}{2} + \cdots + \binom{m}{r}$.

Παρατήρηση 3.4.9. Θα μπορούσαμε να ορίσουμε ως κώδικα Reed-Muller μηδενικής τάξης για $m \geq 0$ τον επαναληπτικό κώδικα $\mathcal{R}_2(2^m)$, οπότε ο Ορισμός 3.4.1 συνάδει με τον γενικό ορισμό των κωδίκων Reed-Muller $r-$τάξης.

Πρόταση 3.4.10. *Για κάθε $m \geq 1$ ο κώδικας $\mathcal{RM}_{m-1}(m)$ αποτελείται από όλα τα στοιχεία του $\mathbb{Z}_2^{2^m}$ αρτίου βάρους. Επομένως για κάθε $r < m$ ο κώδικας $\mathcal{RM}_r(m)$ αποτελείται από στοιχεία αρτίου βάρους.*

Απόδειξη. Επαγωγικά μπορούμε να αποδείξουμε ότι για κάθε $m \geq 2$ και κάθε $1 \leq r \leq m$ ισχύει ότι $\mathcal{RM}_{r-1}(m) \subseteq \mathcal{RM}_r(m)$, άρα γενικά ισχύει $\mathcal{RM}_r(m) \subseteq \mathcal{RM}_{m-1}(m)$ για κάθε $r < m$. Επομένως αν αποδείξουμε το πρώτο μέρος της πρότασης, το υπόλοιπο είναι προφανές.

Προφανώς για $m = 1$ έχουμε ότι ο κώδικας $\mathcal{RM}_0(1) = \{\, 00, 11 \,\}$ αποτελείται από όλες τις λέξεις μήκους 2 αρτίου βάρους. Υποθέτουμε ότι ο κώδικας $\mathcal{RM}_{m-2}(m-1)$ αποτελείται από όλες τις λέξεις μήκους 2^{m-1} αρτίου βάρους. Από τον τρόπο ορισμού των κωδίκων Reed-Muller $(m-1)-$τάξης έχουμε ότι $\mathcal{RM}_{m-1}(m) = \mathcal{RM}_{m-1}(m-1) \oplus \mathcal{RM}_{m-2}(m-1)$. Επομένως ένα στοιχείο του κώδικα $\mathcal{RM}_{m-1}(m)$ είναι της μορφής $\mathbf{u}(\mathbf{u}+\mathbf{v}) = \mathbf{uu} + \mathbf{0v}$ με $\mathbf{u} \in \mathcal{RM}_{m-1}(m-1)$ και $\mathbf{v} \in \mathcal{RM}_{m-2}(m-1)$. Το στοιχείο $\mathbf{uu}$ έχει άρτιο βάρος και το στοιχείο $\mathbf{v}$ έχει άρτιο βάρος από την υπόθεση, επομένως και το στοιχείο $\mathbf{0v}$ έχει άρτιο βάρος. Άρα για το βάρος του στοιχείου $\mathbf{u}(\mathbf{u}+\mathbf{v}) = \mathbf{uu} + \mathbf{0v}$ έχουμε $w(\mathbf{uu}+\mathbf{0v}) = w(\mathbf{uu}) + w(\mathbf{0v}) - 2w(\mathbf{uu} \cap \mathbf{0v})$, το οποίο είναι άρτιο. Η διάσταση του κώδικα $\mathcal{RM}_{m-1}(m)$ είναι ίση με $2^m - 1$ επομένως αποτελείται από όλες τις λέξεις μήκους 2^m αρτίου βάρους.

□

3.4.3 Ασκήσεις

1. Να υπολογίσετε έναν πίνακα ελέγχου ισοτιμίας για τον κώδικα $\mathcal{RM}(2)$ και για τον κώδικα $\mathcal{RM}(3)$.

2. Ποίοι από τους κώδικες Reed-Muller είναι αυτοδυϊκοί; ποίοι είναι μέγιστης απόστασης;

3. Εξετάστε αν ένας Reed-Muller κώδικας ικανοποιεί το άνω φράγμα του Plotkin (Θεώρημα 1.5.24) με ισότητα.

Παράρτημα Α΄

Στοιχεία από την Άλγεβρα

Το Παράρτημα αυτό παρατίθεται για να συμβάλει στην αυτοδυναμία του βιβλίου, στο οποίο ο αναγνώστης θα μπορεί να προστρέχει για αρωγή σε έννοιες και αποτελέσματα που θα συναντά κατά τη μελέτη του πρώτου μέρους. Σε **καμιά** περίπτωση δεν πρέπει να θεωρηθεί ως μια (έστω) σύντομη εισαγωγή σε θέματα Άλγεβρας.

Θεωρούμε γνωστές τις έννοιες της σχέσης ισοδυναμίας, του σώματος, του διανυσματικού χώρου, του δακτυλίου των πολυωνύμων με συντελεστές από ένα σώμα, καθώς και την στοιχειώδη αριθμητική των ακεραίων $\mathrm{mod} n$. [1]

Ο ενδιαφερόμενος αναγνώστης μπορεί **και** πρέπει να ανατρέχει στη σχετική βιβλιογραφία (Ελληνόγλωσση και ξενόγλωσση) για περεταίρω μελέτη σε Αλγεβρικά θέματα, γεγονός που θα τον βοηθήσει να κατανοήσει σε αρκετό βάθος έννοιες του πρώτου μέρους.

Α΄.1 Δακτύλιοι

Α΄.1.1 Ορισμοί και ιδιότητες

Ως γνωστόν ένας δακτύλιος $(\mathrm{R}, +, \cdot)$ είναι ένα μη κενό σύνολο R εφοδιασμένο με δύο πράξεις. Την πρόσθεση και τον πολλαπλασιασμό που πληρούν τις εξής ιδιότητες:

1. Ως προς την πρόσθεση είναι αβελιανή ομάδα, δηλαδή

   (α΄) $a + (b + c) = (a + b) + c$, για όλα τα $a, b, c \in \mathrm{R}$.
   (Η πρόσθεση είναι προσεταιριστική).

[1] Εδώ απλώς θα υπενθυμίσουμε, σε ορισμένες περιπτώσεις, τους βασικούς ορισμούς και θα παραθέσουμε μερικές ιδιότητες.

(β΄) Υπάρχει $0 \in \mathrm{R}$ έτσι ώστε $0 + a = a + 0$ για κάθε $a \in \mathrm{R}$.
(΄Υπαρξη ουδετέρου ως προς την πρόσθεση).

(γ΄) Για κάθε $a \in \mathrm{R}$ υπάρχει $-a \in \mathrm{R}$ έτσι ώστε $a+(-a) = (-a)+a = 0$.
(΄Υπαρξη αντιθέτου ως προς την πρόσθεση).

(δ΄) $a + b = b + a$ για όλα τα $a, b \in \mathrm{R}$.

2. $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ για όλα τα $a, b, c \in \mathrm{R}$.
(Ο πολλαπλασιασμός είναι προσεταιριστικός).

3. $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ και $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$ για όλα τα $a, b, c \in \mathrm{R}$.
(Ο πολλαπλασιασμός είναι επιμεριστικός ως προς την πρόσθεση).

Γνωστά παραδείγματα δακτυλίων είναι:

1. Ο δακτύλιος των ακεραίων $(\mathbb{Z}, +, \cdot)$ με τις γνωστές πράξεις, πρόσθεση και πολλαπλασιασμό, των ακεραίων αριθμών.

2. Ο δακτύλιος $\mathbb{R}[x]$ των πολυωνύμων με συντελεστές πραγματικούς αριθμούς και πράξεις την πρόσθεση και πολλαπλασιασμό πολυωνύμων.

3. Ο δακτύλιος $M_n(\mathbb{R})$ των τετραγωνικών $n \times n$ πινάκων με στοιχεία πραγματικούς αριθμούς και πράξεις την πρόσθεση και πολλαπλασιασμό πινάκων.
Γενικά για κάθε δακτύλιο $(\mathrm{R}, +, \cdot)$ ορίζονται οι αντίστοιχοι δακτύλιοι $\mathrm{R}[x]$ και $M_n(\mathrm{R})$ με τις αντίστοιχες πράξεις.

Ένα άλλο παράδειγμα δακτυλίου είναι ο δακτύλιος $(\mathbb{Z}_m, +, \cdot)$ των ακεραίων $\mathrm{mod}m$ για έναν θετικό ακέραιο m.

Υπενθυμίζουμε πώς ορίζεται ο δακτύλιος $(\mathbb{Z}_m, +, \cdot)$.
Έστω m ένας θετικός ακέραιος. Στο σύνολο των ακεραίων αριθμών ορίζουμε μια σχέση $\sim$ ως εξής:
$a \sim b$ αν και μόνο αν ο m διαιρεί τη διαφορά $a - b$.

Δεν είναι δύσκολο να δούμε ότι η σχέση $\sim$ είναι μια σχέση ισοδυναμίας, η οποία διαμερίζει το σύνολο των ακεραίων σε κλάσεις ισοδυναμίας. Η κλάση ισοδυναμίας ενός ακεραίου αριθμού a είναι το σύνολο
$[a] = \{ r \in \mathbb{Z}, \mid r \sim a \} = \{ r \in \mathbb{Z} \mid \text{με το } m \text{ να διαιρεί τη διαφορά } a - r \} = \{ a + ms \mid s \in \mathbb{Z} \}$. Υπάρχουν τόσες κλάσεις ισοδυναμίας όσα και τα δυνατά υπόλοιπα της διαίρεσης ενός ακεραίου με τον m (γιατί;) Δηλαδή έχουμε τις κλάσεις $[0]$, $[1]$, $\ldots$, $[m-1]$, οι οποίες θα ονομάζονται **κλάσεις υπολοίπων** $\mathrm{mod}m$. Δύο ακέραιοι αριθμοί a, b, οι οποίοι βρίσκονται στην ίδια κλάση ισοδυναμίας, θα λέγονται ισότιμοι ως προς μέτρο m και συμβολίζουμε $a \equiv b \mathrm{mod}m$.

Το σύνολο $\mathbb{Z}_m = \{[0], [1], \ldots, [m-1]\}$ όλων των κλάσεων υπολοίπων mod$m$ είναι οι ακέραιοι mod$m$. Στο $\mathbb{Z}_m$ ορίζουμε δύο πράξεις. Μια πρόσθεση και έναν πολλαπλασιασμό ως εξής:

$[a] + [b] = [a + b]$ και $[a] \cdot [b] = [a \cdot b]$.

Ως άσκηση μπορείτε να διαπιστώσετε ότι οι δύο πράξεις που ορίσαμε είναι "καλά ορισμένες" , δηλαδή αν $[a_1] = [a_2]$, $[b_1] = [b_2]$, τότε $[a_1] + [b_1] = [a_2] + [b_2]$ και $[a_1] \cdot [b_1] = [a_2] \cdot [b_2]$. Με διαφορετικά λόγια, οι πράξεις δεν εξαρτώνται από την επιλογή των αντιπροσώπων,

Το σύνολο $\mathbb{Z}_m$ με τις πράξεις που ορίσαμε προηγουμένως είναι ένας δακτύλιος. (Ως άσκηση να επαληθεύσετε ότι πράγματι το $(\mathbb{Z}_m, +, \cdot)$ είναι δακτύλιος).

Παρατηρήσεις Α΄.1.1. 1. Ο τρόπος που ορίσαμε τις πράξεις στο σύνολο $\mathbb{Z}_m$ "υπαγορεύει" έναν εύκολο τρόπο να εκτελούμε τις πράξεις. Έστω ότι έχουμε να προσθέσουμε/πολλαπλασιάσουμε το $[a]$ με το $[b]$, τότε προσθέτουμε/πολλαπλασιάζουμε το a με το b στους ακεραίους, το αποτέλεσμα που βρίσκουμε το διαιρούμε με τον m και το υπόλοιπο mod$m$ που προκύπτει είναι το αποτέλεσμα της πρόσθεσης/πολλαπλασιασμού του $[a]$ με το $[b]$.
Για παράδειγμα, έστω $[3], [5] \in \mathbb{Z}_6$, τότε $[3] + [5] = [8 = 6 + 2] = [2]$ και $[3] \cdot [5] = [15 = 2 \cdot 6 + 3] = [3]$.

2. Πολλές φορές, όταν δεν υπάρχει ενδεχόμενο σύγχυσης, κάθε κλάση υπολοίπων mod$m$ $[a]$ την ταυτίζουμε με τον αντίστοιχο αντιπρόσωπο a και γράφουμε $\mathbb{Z}_m = \{0, 1, \ldots, m-1\}$.

Ένας δακτύλιος $(\mathrm{R}, +, \cdot)$ θα λέγεται μεταθετικός αν ισχύει $r \cdot s = s \cdot r$ για όλα τα $r, s \in \mathrm{R}$.

Αν σε ένα δακτύλιο $(\mathrm{R}, +, \cdot)$ υπάρχει ουδέτερο ως προς τον πολλαπλασιασμό, δηλαδή υπάρχει $e \in \mathrm{R}$ τέτοιο ώστε $e \cdot r = r \cdot e = r$ για κάθε $r \in \mathrm{R}$, τότε ο δακτύλιος ονομάζεται δακτύλιος με μονάδα και το e τις περισσότερες φορές συμβολίζεται με 1_{R} (ή απλά 1).

Σε όλα τα προηγούμενα παραδείγματα οι δακτύλιοι είναι μεταθετικοί με μονάδα. Εκτός από τον δακτύλιο $M_n(\mathrm{R})$, ο οποίος έχει μονάδα μόνο αν ο δακτύλιος R έχει μονάδα και δεν είναι μεταθετικός για $n > 1$, ακόμα και αν ο δακτύλιος R είναι μεταθετικός.

Σε έναν δακτύλιο R με μονάδα ένα στοιχείο a θα λέγεται ότι έχει αντίστοφο (ή ότι το a είναι αντιστρέψιμο) , αν υπάρχει $a^{-1} \in \mathrm{R}$ έτσι ώστε $a \cdot a^{-1} = a^{-1} \cdot a = 1$. Έστω $U(\mathrm{R})$ σύνολο των αντιστρεψίμων στοιχείων ενός δακτυλίου R. Ως άσκηση μπορείτε να αποδείξετε ότι το γινόμενο δύο αντιστρεψίμων στοιχείων είναι αντιστρέψιμο στοιχείο και ότι το $U(\mathrm{R})$ με πράξη τον πολλαπλασιασμό είναι ομάδα, η **πολλαπλασιαστική ομάδα** του δακτυλίου R.

Προφανώς $U(\mathbb{Z}) = \{1, -1\}$ και $U(M_n(\mathbb{R})) = \{\, \mathrm{A} \in M_n(\mathbb{R}) \mid det(\mathrm{A}) \neq 0\,\}$.

Ως άσκηση θα μπορούσατε να αποδείξετε ότι η πολλαπλασιαστική ομάδα του δακτυλίου των πολυωνύμων $\mathbb{R}[x]$ αποτελείται από τα σταθερά μη μηδενικά πολυώνυμα.

Πρόταση Α΄.1.2. *Έστω m θετικός ακέραιος, το στοιχείο $[a] \in \mathbb{Z}_m$ είναι αντιστρέψιμο αν και μόνο αν ο a είναι πρώτος προς τον m. Δηλαδή $U(\mathbb{Z}_m) = \{\, [a] \in \mathbb{Z}_m \mid \mu.\kappa.\delta.(a, m) = 1\,\}$.*

Απόδειξη. Υποθέτουμε ότι ο $[a] \in \mathbb{Z}_m$ είναι αντιστρέψιμος δηλαδή υπάρχει $[b] \in \mathbb{Z}_m$ έτσι ώστε $[a] \cdot [b] = [1]$, αυτό σημαίνει ότι $ab \equiv 1 \mathrm{mod} m$, δηλαδή ο m διαιρεί τη διαφορά $ab - 1$. Οπότε έχουμε ότι υπάρχει ακέραιος k τέτοιος ώστε $ab - 1 = mk$, δηλαδή $ab - mk = 1$ απ' όπου έπεται ότι ο μέγιστος κοινός διαιρέτης των a και m ισούται με 1.

Αντίστροφα, υποθέτουμε ότι ο a είναι πρώτος προς τον m, τότε υπάρχουν ακέραιοι k, n, έτσι ώστε $ak + mn = 1$ [2]. Από την τελευταία σχέση έπεται ότι $ak \equiv 1 \mathrm{mod} m$, δηλαδή $[a][k] = [1]$, άρα το $[a]$ είναι αντιστρέψιμο στοιχείο του $\mathbb{Z}_m$.

□

Ένα μη κενό υποσύνολο S ενός δακλτυλίου R θα λέγεται **υποδακτύλιος** αν είναι δακτύλιος ως προς την πρόσθεση και τον πολλαπλασιασμό του δακτυλίου R. Δηλαδή το S είναι υποομάδα ως προς την πρόσθεση και $a \cdot b \in \mathrm{S}$ για κάθε $a, b \in \mathrm{S}$.

Επισημαίνουμε ότι το μηδέν (το ουδέτερο της πρόσθεσης) ενός δακτυλίου ανήκει σε **κάθε** υποδακτύλιο (γιατί;). Για την μονάδα (το ουδέτερο του πολλαπλασιασμού) δεν ισχύει κάτι ανάλογο.

1. Ο δακτύλιος των ακεραίων έχει μονάδα. Έστω m ένας θετικός ακέραιος μεγαλύτερος του 1, το σύνολο $m\mathbb{Z} = \{\, m \cdot r \mid r \in \mathbb{Z}\,\}$ είναι υποδακτύλιος του $\mathbb{Z}$, αλλά δεν έχει μονάδα ως προς τον πολλαπλασιασμό.

2. Το σύνολο $\mathrm{R}\{\begin{pmatrix} r & 0 \\ 0 & 0 \end{pmatrix} \mid r \in \mathbb{Z}\}$ αποτελεί υποδακτύλιο του δακτυλίου $M_2(\mathbb{Z})$ των τετραγωνικών 2×2 πινάκων με στοιχεία ακεραίους αριθμούς.

[2] Εδώ χρησιμοποιούμε (χωρίς απόδειξη) το εξής βασικό θεώρημα της Θεωρίας Αριθμών: Έστω α, β ακέραιοι αριθμοί όχι και οι δύο ίσοι με μηδέν, τότε υπάρχουν ακέραιοι κ, λ έτσι ώστε $\mu.\kappa.\delta.(\alpha, \beta) = \alpha\kappa + \beta\lambda$.

Ο R έχει ως μονάδα τον πίνακα $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, ενώ ο $M_2(\mathbb{Z})$ έχει ως μονάδα τον πίνακα $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

Σε έναν δακτύλιο R ένα μη μηδενικό στοιχείο a θα λέγεται **διαιρέτης του μηδενός** αν υπάρχουν μη μηδενικά $b, c \in \mathrm{R}$ έτσι ώστε $ab = ca = 0$.
Σε έναν δακτύλιο με μονάδα ένα αντιστρέψιμο στοιχείο δεν είναι διαιρέτης του μηδενός (γιατί;).

Ένας μεταθετικός δακτύλιος με μονάδα και δύο τουλάχιστον στοιχεία θα λέγεται **ακεραία περιοχή** αν δεν έχει διαιρέτες του μηδενός.

Ο δακτύλιος των ακεραίων είναι προφανώς ακεραία περιοχή. Επίσης ο δακτύλιος $\mathbb{R}[x]$ των πολυωνύμων με πραγματικούς συντελεστές είναι ακεραία περιοχή (γιατί;). Γενικά αν R είναι ένας δακτύλιος, τότε μπορείτε να αποδείξετε ότι ο $\mathrm{R}[x]$ είναι ακεραία περιοχή αν και μόνο αν ο R είναι ακεραία περιοχή.

Ο δακτύλιος όμως $M_n(\mathrm{R})$ δεν είναι ακεραία περιοχή για $n > 1$. Για παράδειγμα, για τους πίνακες $\mathrm{A} = \begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix}$ και $\mathrm{B} = \begin{pmatrix} 0 & 2 \\ 0 & 0 \end{pmatrix}$ έχουμε ότι $\mathrm{B} \cdot \mathrm{A} = \mathbf{0}$.

Πρόταση Α΄.1.3. *Ο δακτύλιος $\mathbb{Z}_m$ είναι ακεραία περιοχή αν και μόνο αν ο m είναι πρώτος αριθμός.*

Απόδειξη. Δίνουμε μια σκιαγράφηση της απόδειξης με τις λεπτομέρειες να αφίνονται ως άσκηση.

Αρκεί να παρατηρήσουμε ότι αν $m = a \cdot b$ με a, b διάφορα του 1, τότε τα $[a]$, $[b] \in \mathbb{Z}_m$ είναι διαιρέτες του μηδενός.

Αντίστροφα, αν τα $[a]$, $[b] \in \mathbb{Z}_m$ είναι διαιρέτες του μηδενός και ισχύει $[a] \cdot [b] = [0]$, τότε έχουμε ότι ο m διαιρεί το γινόμενο ab, οπότε αν ο m ήταν πρώτος θα έπρεπε να διαιρεί (τουλάχιστον) έναν από τους a, b. Άρα ένας από τους $[a]$, $[b]$ θα ήταν ίσος με $[0]$, άτοπο.

□

Ως άσκηση θα μπορούσατε να υπολογίσετε τους διαιρέτες του μηδενός στο δακτύλιο $\mathbb{Z}_m$.

Έστω R ένας δακτύλιος, ο μικρότερος θετικός ακέραιος n (αν υπάρχει) με την ιδιότητα $nr = \underbrace{r + r + \cdots + r}_{n-\text{φορές}} = 0$ για ολα τα $r \in \mathrm{R}$ θα λέγεται **χαρακτηριστική** του δακτυλίου . Αν δεν υπάρχει θετικός ακέραιος με την παραπάνω ιδιότητα, τότε θα λέμε ότι η χαρακτηριστική του δακτυλίου ισούται με μηδέν.

Προφανώς η χαρακτηριστική του δακτυλίου $\mathbb{Z}$ των ακεραίων είναι ίση με μηδέν. Ενώ η χαρακτηριστική του δακτυλίου $\mathbb{Z}_m$ είναι ίση με m.

Πρόταση Α΄.1.4. *Η χαρακτηριστική μιας ακεραίας περιοχής D είναι είτε μηδέν είτε πρώτος αριθμός.*

Απόδειξη. Υποθέτουμε ότι η χαρακτηριστική της D δεν είναι μηδέν και είναι ίση με m. Παρατηρούμε ότι ο m είναι ο ελάχιστος θετικός ακέραιος τέτοιος ώστε $m1 = 0$. Πράγματι, αν υπήρχε $0 < n < m$ με $n1 = 0$, τότε για κάθε $a \in D$ θα είχαμε ότι $na = (n1) \cdot a = 0$. Αυτό είναι άτοπο από τον ορισμό της χαρακτηριστικής.

Αν ο m είναι σύνθετος, τότε θα έχουμε $m = r \cdot s$ με $1 < r, s < m$. Οπότε $(r1) \cdot (s1) = (r \cdot s)1 = m1 = 0$ και επειδή η D είναι ακεραία περιοχή έχουμε ότι $r1 = 0$ ή $s1 = 0$, άτοπο από τα προηγούμενα.

□

Ένας μεταθετικός δακτύλιος $\mathbb{F}$ με μονάδα όπου κάθε μη μηδενικό στοιχείο του έχει αντίστροφο λέγεται **σώμα** . Δηλαδή η πολλαπλασιαστική ομάδα ενός σώματος αποτελείται από όλα τα μη μηδενικά στοιχεία του.

Τα σύνολα $\mathbb{Q}$ των ρητών, $\mathbb{R}$ των πραγματικών και $\mathbb{C}$ των μιγαδικών αριθμών είναι σώματα με τις συνήθεις πράξεις πρόσθεσης και πολλαπλασιασμού.

Προφανώς κάθε σώμα είναι ακεραία περιοχή. Το αντίστροφο προφανώς δεν ισχύει, αφού ο δακτύλιος των ακεραίων είναι ακεραία περιοχή, αλλά δεν είναι σώμα.

Αν η ακεραία περιοχή είναι πεπερασμένη, τότε ισχύει και το αντίστροφο. Συγκεκριμμένα έχουμε.

Πρόταση Α΄.1.5. *Κάθε πεπερασμένη ακεραία περιοχή D είναι σώμα.*

Απόδειξη. Για κάθε $0 \neq a \in D$ και κάθε θετικό ακέραιο λ οι δυνάμεις a^λ είναι στοιχεία της D και επειδή η D είναι πεπερασμένη υπάρχουν κ, λ θετικοί ακέραιοι με $\kappa < \lambda$ και $a^\kappa = a^\lambda$. Δηλαδή έχουμε ότι $a^\kappa - a^\lambda = 0$, οπότε έχουμε $a^\kappa(1 - a^{\lambda-\kappa}) = 0$. Επειδή η D είναι ακεραία περιοχή έχουμε ότι $1 - a^{\lambda-\kappa} = 0$. Από την τελευταία σχέση έχουμε ότι $a^{\lambda-\kappa} = 1$, απ' όπου έπεται ότι το a είναι αντιστρέψιμο στοιχείο.

□

Ανακεφαλαιώνοντας τα προηγούμενα μπορούμε να αποδείξουμε:

1. Ένα στοιχείο του δακτυλίου $\mathbb{Z}_m$ είναι διαιρέτης του μηδενός αν και μόνο αν είναι αντιστρέψιμο.

2. Ο δακτύλιος $\mathbb{Z}_m$ είναι ακεραία περιοχή αν και μόνο αν ο m είναι πρώτος αν και μόνο αν ο $\mathbb{Z}_m$ είναι σώμα.

Α΄.1.2 Ομομορφισμοί-Ιδεώδη

Έστω R_1 και R_2 δύο δακτύλιοι. Μια απεικόνιση $f : \mathrm{R}_1 \longrightarrow \mathrm{R}_2$ θα λέγεται **ομομορφισμός δακτυλίων** αν για όλα τα $a, b \in \mathrm{R}_1$ ισχύει

1. $f(a+b) = f(a) + f(b)$
2. $f(a \cdot b) = f(a) \cdot f(b)$

Δηλαδή ένας ομομορφισμός δακτυλίων " διατηρεί" τις πράξεις των δακτυλίων.

Προφανώς η απεικόνιση $\vartheta : \mathrm{R}_1 \longrightarrow \mathrm{R}_2$ με $\vartheta(r) = 0$ για κάθε $r \in \mathrm{R}_1$ είναι προφανώς ένας ομομορφισμός δακτυλίων, ο **τετριμμένος ομομορφισμός**.

Η απεικόνιση $\varphi : \mathbb{Z} \longrightarrow \mathbb{Z}_m$ με $\varphi(a) = [a]$ για κάθε $a \in \mathbb{Z}$ είναι προφανώς ένας ομομορφισμός δακτυλίων, **φυσικός ομομορφισμός**.

Στη συνέχεια θα μας δοθεί η ευκαιρία να δούμε περισσότερα παραδείγματα ομομορφισμών δακτυλίων.

Έστω $f : \mathrm{R}_1 \longrightarrow \mathrm{R}_2$ ένας ομομορφισμός δακτυλίων τότε ισχύει $f(0) = 0$ (γιατί;).

Το σύνολο $f(\mathrm{R}_1) = \{\, f(a) \in \mathrm{R}_2 \mid a \in \mathrm{R}_1 \,\}$ είναι υποδακτύλιος του R_2 (γιατί;), συνήθως συμβολίζεται $\mathrm{Im}f$ και ονομάζεται **δακτύλιος εικόνα**.
Όταν η απεικόνιση f είναι επί, τότε προφανώς $\mathrm{Im}f = \mathrm{R}_2$ και η f ονομάζεται **επιμορφισμός**.

Το σύνολο $\{\, r \in \mathrm{R}_1 \mid f(r) = 0 \,\}$ ονομάζεται **πυρήνας** της f και συμβολίζεται $\mathrm{Ker}f$.

Ο φυσικός ομομορφισμός $\varphi : \mathbb{Z} \longrightarrow \mathbb{Z}_m$ με $\varphi(a) = [a]$ είναι προφανώς επί και έχει πυρήνα $\mathrm{Ker}\varphi = \{\, mr \mid r \in \mathbb{Z} \,\}$ (γιατί;)

Προφανώς ο πυρήνας του τετριμμένου ομομορφισμού $\vartheta : \mathrm{R}_1 \longrightarrow \mathrm{R}_2$ με $\vartheta(r) = 0$ για κάθε $r \in \mathrm{R}_1$ είναι όλος ο δακτύλιος $\mathbb{R}_1$.

Πρόταση Α΄.1.6. *Ο ομομορφισμός δακτυλίων $f : \mathrm{R}_1 \longrightarrow \mathrm{R}_2$ είναι 1 - 1 αν και μόνο αν $\mathrm{Ker}f = \{\, 0 \,\}$.*

Απόδειξη. Για $a, b \in \mathbb{R}_1$ ισχύει $f(a) = f(b)$ αν και μόνο αν $f(a) - f(b) = f(a-b) = 0$ αν και μόνο αν $a - b \in \mathrm{Ker}f$. Οπότε η συνέχεια έπεται εύκολα. □

Αν ένας ομομορφισμός δακτυλίων είναι 1 - 1, τότε ονομάζεται **μονομορφισμός**. Αν είναι 1 - 1 και επί, ονομάζεται **ισομορφισμός**.

Έστω $(\mathrm{R}, +, \cdot)$ ένας δακτύλιος και I ένα μη κενό υποσύνολο του R. Το I θα λέγεται **ιδεώδες** του R (και θα συμβολίζεται $\mathrm{I} \lhd \mathrm{R}$) αν ισχύουν:

i) $a - b \in \mathrm{I}$, για όλα τα $a, b \in \mathrm{I}$.

ii) $r \cdot a,\ a \cdot r \in \mathrm{I}$, για όλα τα $a \in \mathrm{I}$ και $r \in \mathrm{R}$.

Προφανώς το σύνολο $\{0\}$ που αποτελείται μόνο από το μηδέν είναι ιδεώδες και ονομάζεται το **μηδενικό** ή το τετριμμένο ιδεώδες. Επίσης ολόκληρος ο δακτύλιος R είναι ιδεώδες του εαυτού του. Ένα ιδεώδες I με $\{0\} \neq \mathrm{I} \neq \mathrm{R}$ θα λέγεται **γνήσιο** ιδεώδες.

Όπως βλέπουμε ένα ιδεώδες είναι "κάτι περισσότερο" από υποδακτύλιος. Για παράδειγμα στο δακτύλιο $\mathbb{Q}[x]$ όλων των πολυωνύμων με ρητούς συντελεστές το σύνολο $\mathbb{Z}[x]$ όλων των πολυωνύμων με ακεραίους συντελεστές είναι υποδακτύλιος, αλλά δεν είναι ιδεώδες (γιατί;). Ενώ το σύνολο K όλων των πολυωνύμων με μηδενικό σταθερό όρο είναι ιδεώδες (γιατί;)

Στο δακτύλιο των ακεραίων $\mathbb{Z}$ μπορείτε ως άσκηση να αποδείξετε ότι για κάθε ιδεώδες I υπάρχει ένας θετικός ακέραιος m έτσι ώστε $\mathrm{I} = m\mathbb{Z} = \{m \cdot r \mid r \in \mathbb{Z}\}$. Ως υπόδειξη μπορείτε να πάρετε (στην περίπτωση που το I είναι μη μηδενικό) τον μικρότερο θετικό ακέραιο $m \in \mathrm{I}$ και να αποδείξετε ότι διαιρεί κάθε άλλο στοιχείο του I.

Έστω I_1, I_2 ιδεώδη του δακτυλίου R, τότε μπορούμε εύκολα να αποδείξουμε ότι η τομή $\mathrm{I}_1 \cap \mathrm{I}_2$ είναι ιδεώδες του R.
Για παράδειγμα μπορείτε να αποδείξετε ότι αν $\mathrm{I}_1 = \{m \cdot r \mid r \in \mathbb{Z}\}$ και $\mathrm{I}_2 = \{n \cdot r \mid r \in \mathbb{Z}\}$ είναι δύο ιδεώδη του δακτυλίου των ακεραίων , τότε $\mathrm{I}_1 \cap \mathrm{I}_2 = \{k \cdot r \mid r \in \mathbb{Z}\}$, όπου k είναι το ελάχιστο κοινό πολλαπλάσιο των m και n.

Όπως εύκολα μπορούμε να διαπιστώσουμε η ένωση δύο ιδεωδών δεν είναι κατ' ανάγκη ιδεώδες.
Μπορείτε να αποδείξετε ότι η ένωση $\mathrm{I}_1 \cup \mathrm{I}_2$ είναι ιδεώδες του R αν και μόνο αν $\mathrm{I}_1 \subseteq \mathrm{I}_2$ ή $\mathrm{I}_1 \supseteq \mathrm{I}_2$.

Έστω R ένας δακτύλιος και $S \subseteq \mathrm{R}$. Η τομή όλων των ιδεωδών του R που περιέχουν το υποσύνολο S είναι το μικρότερο ιδεώδες του R που περιέχει το υποσύνολο S, ονομάζεται **ιδεώδες παραγόμενο** από το υποσύνολο S και συμβολίζεται $\langle S \rangle$. Δηλαδή $\langle S \rangle = \bigcap\{\mathrm{I} \mid \mathrm{I} \lhd \mathrm{R}\ \textit{και}\ S \subseteq \mathrm{I}\}$.

Έστω I_1, I_2 δύο ιδεώδη του δακτυλίου R, Δεν είναι δύσκολο να αποδείξουμε ότι $\langle \mathrm{I}_1 \cup \mathrm{I}_2 \rangle = \{a + b \mid a \in \mathrm{I}_1,\ b \in \mathrm{I}_2\}$. Για το λόγο αυτό το ιδεώδες $\{a+b \mid a \in \mathrm{I}_1,\ b \in \mathrm{I}_2\}$ το συμβολίζουμε με $\mathrm{I}_1+\mathrm{I}_2$ και το ονομάζουμε **άθροισμα** των ιδεωδών I_1 και I_2.

Πρόταση Α΄.1.7. *Έστω* R *ένας μεταθετικός δακτύλιος με μονάδα και* $\emptyset \neq S \subseteq \mathrm{R}$, *τότε* $\langle S \rangle = \{a_1 s_1 + a_2 s_2 + \cdots + a_\nu s_\nu \mid a_i \in \mathrm{R},\ s_i \in S,$ $i = 1, 2, \ldots, \nu,\ \nu \geq 1\}$.

Απόδειξη. Το σύνολο $\{a_1 s_1 + a_2 s_2 + \cdots + a_\nu s_\nu \mid a_i \in \mathrm{R},\ s_i \in S,$ $i = 1, 2, \ldots, \nu,\ \nu \geq 1\}$ είναι ιδεώδες του R (γιατί;). Επίσης το υποσύνολο S

περιέχεται στο $\{\, a_1s_1 + a_2s_2 + \cdots + a_\nu s_\nu \mid a_i \in \mathrm{R},\ s_i \in S,$
$i = 1, 2, \ldots, \nu,\ \nu \geq 1 \,\}$. Επομένως από τον ορισμό του $\langle S \rangle$ έχουμε ότι
$\langle S \rangle \subseteq \{\, a_1s_1 + a_2s_2 + \cdots + a_\nu s_\nu \mid a_i \in \mathrm{R},\ s_i \in S,\ i = 1, 2, \ldots, \nu,\ \nu \geq 1 \,\}$.

Έστω τώρα I ένα ιδεώδες του R με $S \subseteq \mathrm{I}$. Από τον ορισμό του ιδεώδους έπεται ότι
$\{\, a_1s_1 + a_2s_2 + \cdots + a_\nu s_\nu \mid a_i \in \mathrm{R},\ s_i \in S,\ i = 1, 2, \ldots, \nu,\ \nu \geq 1 \,\} \subseteq \mathrm{I}$.
Δηλαδή $\{\, a_1s_1 + a_2s_2 + \cdots + a_\nu s_\nu \mid a_i \in \mathrm{R},\ s_i \in S,$
$i = 1, 2, \ldots, \nu,\ \nu \geq 1 \,\} \subseteq \bigcap \{\, \mathrm{I} \mid \mathrm{I} \lhd \mathrm{R}\ \textit{και}\ S \subseteq \mathrm{I} \,\} = \langle S \rangle$ και τελειώσαμε.

□

Παρατηρήσεις Α΄.1.8. 1. Αν $S = \emptyset$, τότε προφανώς $\langle \emptyset \rangle = \{\, 0 \,\}$.

2. Στη γενική περίπτωση, όπου ο δακτύλιος δεν είναι κατ' ανάγκη μεταθετικός, ούτε έχει κατ' ανάγκη μονάδα, μπορούμε επίσης να περιγράψουμε τα στοιχεία ενός ιδεώδους που παράγεται από ένα υποσύνολο του δακτυλίου. Αρκεστήκαμε όμως στην μερική περίπτωση, διότι στα επόμενα θα ασχοληθούμε, χωρίς ιδιαίτερη μνεία, αποκλειστικά με μεταθετικούς δακτυλίους με μονάδα.

Ενδιαφέρον παρουσιάζει η περίπτωση που το υποσύνολο S αποτελείται από ένα στοιχείο.
Αν R είναι ένας δακτύλιος και $a \in \mathrm{R}$, τότε το ιδεώδες το παραγόμενο από το μονοσύνολο $\{\, a \,\}$ θα ονομάζεται **κύριο** και προφανώς ισχύει $\langle \{\, a \,\} \rangle = \langle\, a \,\rangle =$
$= \{\, r \cdot a \mid r \in \mathrm{R} \,\}$.

Προηγουμένως έχουμε δει ότι για κάθε ιδεώδες I του δακτυλίου των ακεραίων υπάρχει ένας θετικός ακέραιος m έτσι ώστε $\mathrm{I} = m\mathbb{Z} = \{\, m \cdot r \mid r \in \mathbb{Z} \,\}$. Δηλαδή το $\mathrm{I} = \langle\, m \,\rangle$ είναι κύριο. Άρα κάθε ιδεώδες του δακτυλίου $\mathbb{Z}$ είναι κύριο. Γενικά αν σε ένα δακτύλιο κάθε ιδεώδες του είναι κύριο, τότε ο δακτύλιος θα ονομάζεται **δακτύλιος κυρίων ιδεωδών** . Στα επόμενα θα δούμε και άλλα παραδείγματα δακτυλίων κυρίων ιδεωδών.

Έστω R ένας δακτύλιος και I ένα ιδεώδες του. Υποθέτουμε ότι το $1 \in \mathrm{I}$, τότε προφανώς (από τον ορισμό του ιδεώδους) έχουμε ότι $\mathrm{I} = \mathrm{R}$.
Από την απλή αυτή παρατήρηση έπεται άμεσα ότι $\langle\, a \,\rangle = \mathrm{R}$ αν και μόνο αν το στοιχείο $a \in \mathrm{R}$ είναι αντιστρέψιμο (γιατί;) .
Επίσης από την ίδια παρατήρηση έπεται άμεσα ότι σε ένα σώμα τα μόνα ιδεώδη του είναι το μηδενικό ιδεώδες και ολόκληρο το σώμα (γιατί;) .

Έστω $f : \mathrm{R}_1 \longrightarrow \mathrm{R}_2$ ένας ομομορφισμός δακτυλίων. Υποθέτουμε ότι
$a, b \in \mathrm{Ker} f$, τότε δεν είναι δύσκολο να δούμε ότι $a - b \in \mathrm{Ker} f$, όπως επίσης ότι για κάθε $r \in \mathrm{R}_1$ τα $r \cdot a,\ a \cdot r \in \mathrm{R}_1$. Δηλαδή ισχύει η εξής πρόταση.

Πρόταση Α΄.1.9. *Ο πυρήνας ένος ομομορφισμού δακτυλίων είναι ιδεώδες του πεδίου ορισμού.*

Παράδειγμα Α΄.1.10. Έστω $\mathbb{F}[x]$ ο δακτύλιος των πολυωνύμων με συντελεστές από το σώμα $\mathbb{F}$ και $\varphi : \mathbb{F}[x] \longrightarrow \mathbb{F}[x]$ με $\varphi(a_n x^n + \cdot + a_1 x + a_0) = a_0$, δηλαδή η απεικόνιση φ απεικονίζει κάθε πολυώνυμο στον σταθερό του όρο. Δεν είναι δύσκολο να αποδείξουμε ότι η φ είναι ομομορφισμός δακτυλίων. Επίσης μπορείτε να αποδείξετε ότι ο πυρήνας της φ είναι όλα τα πολυώνυμα με μηδενικό σταθερό πολυώνυμο. Επομένως, σύμφωνα με τα προηγούμενα, το σύνολο των πολυωνύμων με μηδενικό σταθερό όρο είναι ένα ιδεώδες του $\mathbb{F}[x]$.

Όπως θα δούμε αμέσως ισχύει και το αντίστροφο της προηγούμενης πρότασης, δηλαδή κάθε ιδεώδες είναι ο πυρήνας ενός ομομορφισμού δακτυλίων. Οπότε οι έννοιες πυρήνας ομομορφισμού και ιδεώδες είναι ταυτόσημες.

Έστω I ένα ιδεώδες του δακτυλίου R. Στο δακτύλιο R ορίζουμε μια σχέση $\sim$ ως εξής: $a \sim b$ αν και μόνο αν $a - b \in \mathrm{I}$.

Ως άσκηση μπορείτε να αποδείξετε ότι η σχέση $\sim$ είναι σχέση ισοδυναμίας. Ας υπολογίσουμε τις κλάσεις ισοδυναμίας. Η κλάση ισοδυναμίας του στοιχείου a είναι το σύνολο $C_a = \{\, r \in \mathrm{R} \mid r - a \in \mathrm{I} \,\} = \{\, r \in \mathrm{R} \text{ } \textit{για τα οποία υπάρχει } h \in \mathrm{I} \text{ } \textit{έτσι ώστε} \text{ } r = a + h \,\} = \{\, a + h \mid h \in \mathrm{I} \,\}$. Την κλάση $C_a = \{\, a + h \mid h \in \mathrm{I} \,\}$ θα την ονομάζουμε **σύμπλοκο** ή **κλάση υπολοίπων** του a ως προς το ιδεώδες I και θα συμβολίζεται $a + \mathrm{I}$.

Το σύνολο $\{\, a + \mathrm{I} \mid a \in \mathrm{R} \,\}$ όλων των συμπλόκων αποτελεί το σύνολο πηλίκων ως προς τη σχέση ισοδυναμίας $\sim$ και θα συμβολίζεται R/I.

Με τη βοήθεια των πράξεων της πρόσθεσης και του πολλαπλασιασμού στο δακτύλιο R, στο σύνολο R/I ορίζουμε δύο πράξεις, μια πρόσθεση και έναν πολλαπλασιασμό ως εξής:

$(a + \mathrm{I}) + (b + \mathrm{I}) = (a + b) + \mathrm{I}$

$(a + \mathrm{I}) \cdot (b + \mathrm{I}) = (a \cdot b) + \mathrm{I}$

Δεν είναι δύσκολο να αποδείξουμε ότι οι δύο πράξεις είναι καλά ορισμένες (δεν εξαρτώνται από την επιλογή των αντιπροσώπων).

Ως άσκηση μπορείτε να αποδείξετε ότι το σύνολο R/I με αυτές τις πράξεις αποτελεί δακτύλιο. (Το μηδέν, δηλαδή το ουδέτερο ως προς την πρόσθεση, είναι το σύμπλοκο $0 + \mathrm{I} = \mathrm{I}$). Ο δακτύλιος αυτός ονομάζεται **δακτύλιος πηλίκων** ως προς το ιδεώδες I.

Παρατήρηση Α΄.1.11. Ο δακτύλιος των ακεραίων $\mathbb{Z}_m$ των ακεραίων $\mathrm{mod}m$ (βλεπε σελίδα 156) είναι ο δακτύλιος πηλίκων $\mathbb{Z}/\langle\, m \,\rangle$.

Έστω $\varphi : \mathrm{R} \longrightarrow \mathrm{R/I}$ η (φυσική) απεικόνιση με $\varphi(r) = r + \mathrm{I}$. Η φ είναι επιμορφισμός δακτυλίων (γιατί;) με $\mathrm{Ker}\varphi = \mathrm{I}$ (γιατί;). Άρα βλέπουμε ότι για

το ιδεώδες I υπάρχει ένας ομομορφισμός δακτυλίων του οποίου ο πυρήνας είναι το I.

Θεώρημα Α΄.1.12. 1^0 Θεώρημα ισομορφισμών
Έστω $\varphi : \mathrm{R}_1 \longrightarrow \mathrm{R}_2$ ομομορφισμός δακτυλίων. Τότε υπάρχει $\overline{\varphi} : \mathrm{R}_1/Ker\varphi \longrightarrow \mathrm{Im}\varphi$ ισομορφισμός δακτυλίων.

Απόδειξη. Για κάθε $r + Ker\varphi \in \mathrm{R}_1/Ker\varphi$ ορίζουμε $\overline{\varphi}(r + Ker\varphi) = \varphi(r)$.

Ως άσκηση μπορείτε να αποδείξετε ότι η $\overline{\varphi}$ είναι ομομορφισμός δακτυλίων 1 - 1 και επί (βλέπε Πρόταση Α΄.1.6 και τον ορισμό του δακτυλίου πηλίκων).

□

Α΄.1.3 Επεκτάσεις σωμάτων

Έστω $\mathbb{F}$ ένα σώμα και $\mathbb{E}$ ένα σώμα που περιέχει το $\mathbb{F}$ ως υπόσωμα. Το $\mathbb{E}$ ονομάζεται **επέκταση** του $\mathbb{F}$ και συμβολίζεται $\mathbb{F} \leq \mathbb{E}$ ή $\mathbb{F} \mid \mathbb{E}$.

Έστω $\mathbb{E}$ μια επέκταση του σώματος $\mathbb{F}$, τότε το σώμα $\mathbb{E}$ μπορεί να θεωρηθεί ως διανυσματικός χώρος επί του σώματος $\mathbb{F}$, όπου η πρόσθεση είναι η πρόσθεση του σώματος $\mathbb{E}$ και ο αριθμητικός πολλαπλασιασμός είναι ο πολλαπλασιασμός ενός στοιχείου του σώματος $\mathbb{F}$ και ενός στοιχείου του σώματος $\mathbb{E}$.
Η διάσταση του $\mathbb{E}$ ως διανυσματικού χώρου επί του $\mathbb{F}$ ονομάζεται **βαθμός** επέκτασης και συμβολίζεται $[\mathbb{E} : \mathbb{F}]$. Αν οβαθμός επέκτασης είναι πεπερασμένος, τότε η επέκταση $\mathbb{F} \mid \mathbb{E}$ λέγεται πεπερασμένη επέκταση, διαφορετικά λέγεται άπειρη.
Για παράδειγμα, αν $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ είναι τα σώματα των ρητών, των πραγματικών και των μιγαδικών αριθμών αντίστοιχα, τότε $[\mathbb{C} : \mathbb{R}] = 2$ ενώ $[\mathbb{R} : \mathbb{Q}] = \infty$.

Έστω $\mathbb{F} \leq \mathbb{K} \leq \mathbb{E}$, τότε μπορούμε να αποδείξουμε (προσπαθήστε το!) ότι $[\mathbb{E} : \mathbb{F}] = [\mathbb{E} : \mathbb{K}] \cdot [\mathbb{K} : \mathbb{F}]$.

Έστω $\mathbb{F}$ ένα σώμα χαρακτηριστικής μηδέν και $\mathbb{Q}$ το σώμα των ρητών αριθμών. Ορίζουμε την απεικόνιση $\varphi : \mathbb{Q} \longrightarrow \mathbb{F}$ ως εξής: $\varphi(a/b) = (a \cdot 1) \cdot (b^{-1} \cdot 1)$, όπου $1 \in \mathbb{F}$ είναι το μοναδιαίο του σώματος $\mathbb{F}$.
Μπορείτε να αποδείξετε ότι η απεικόνιση φ είναι ένας ομομορφισμός σωμάτων μάλιστα δε είναι 1 - 1.

Έστω $\mathbb{F}$ ένα σώμα χαρακτηριστικής p και $\mathbb{Z}_p$ το σώμα των ακεραίων $\mathrm{mod}p$. Ορίζουμε την απεικόνιση $\vartheta : \mathbb{Z}_p \longrightarrow \mathbb{F}$ ως εξής: $\vartheta([a]) = \underbrace{1 + 1 + \cdots + 1}_{a-\text{φορές}}$, όπου 1 είναι το μοναδιαίο του σώματος $\mathbb{F}$.
Μπορείτε να αποδείξετε ότι η απεικόνιση φ είναι ένας ομομορφισμός σωμάτων μάλιστα δε είναι 1 - 1.

Πρόταση Α΄.1.13. *Κάθε σώμα χαρακτηριστικής περιέχει ένα υπόσωμα ισόμορφο με το σώμα των ρητών αριθμών.*

Κάθε σώμα χαρακτηριστικής p περιέχει ένα υπόσωμα ισόμορφο με το σώμα $\mathbb{Z}_p$.

Απόδειξη. Ως άσκηση μπορείτε να αποδείξετε ότι οι απεικονίσεις φ και ϑ που ορίσαμε προηγουμένως είναι πράγματι ομομορφισμοί και 1 - 1, οπότε το αποτέλεσμα είναι άμεσο. □

Πόρισμα Α΄.1.14. *Το σώμα των ρητών αριθμών είναι (μέσω ισομορφισμού) το μικρότερο υπόσωμα ένος σώματος χαρακτηριστικής μηδέν.*

Το σώμα των ακεραίων mod$p$ *είναι (μέσω ισομορφισμού) το μικρότερο υπόσωμα ένος σώματος χαρακτηριστικής p.*

Απόδειξη. Η τομή υποσωμάτων ενός σώματος είναι σώμα (γιατί;). Επομένως η τομή όλων των υποσωμάτων ενός σώματος είναι υπόσωμα, το οποίο στην περίπτωση που η χαρακτηριστική του σώματος είναι μηδέν περιέχει και περιέχεται στο $\mathbb{Q}$ (γιατί;). Ενώ στην περίπτωση που η χαρακτηριστική του σώματος είναι p περιέχει και περιέχεται στο $\mathbb{Z}_p$.

□

Από τα προηγούμενα συνάγουμε τον επόμενο ορισμό.

Το σώμα των ρητών αριθμών και το σώμα $\mathbb{Z}_p$ ονομάζονται **πρώτα** σώματα .

Έστω $\mathbb{F} \leq \mathbb{E}$ μια επέκταση του σώματος $\mathbb{F}$ και $c \in \mathbb{E}$, ορίζουμε $\mathbb{F}(c) = \bigcap\{\, \mathbb{K} \mid \mathbb{K} \leq \mathbb{E}$ με $\mathbb{F} \subseteq \mathbb{K}$ και $c \in \mathbb{K}\,\}$. Δηλαδή το $\mathbb{F}(c)$ είναι το μικρότερο σώμα του $\mathbb{E}$ που περιέχει το σώμα $\mathbb{F}$ και το στοιχείο c.
Το σώμα $\mathbb{F}(c)$ ονομάζεται επέκταση του $\mathbb{F}$ με προσάρτηση του στοιχείου c.

Προφανώς μπορούμε να προσαρτήσουμε περισσότερα του ενός στοιχεία σε ένα σώμα. Μάλιστα δε ισχύει: Αν $c_1, c_2 \in \mathbb{E}$, τότε $(\mathbb{F}(c_1))(c_2) = (\mathbb{F}(c_2))(c_1)$ (γιατί;). Επομένως μπορούμε να γράφουμε $\mathbb{F}(c_1, c_2)$.

Για παράδειγμα προσαρτώντας το $\sqrt{2}$ στο $\mathbb{Q}$ έχουμε το σώμα $\mathbb{Q}(\sqrt{2}) = \{\, a + b\sqrt{2} \mid a, b \in \mathbb{Q}\,\}$. (Γιατί στα στοιχεία του $\mathbb{Q}(\sqrt{2})$ είναι αυτής της μορφής;)

Α΄.2 Ο δακτύλιος των πολυωνύμων

Έστω $\mathbb{F}$ ένα σώμα και $\mathbb{F}[x]$ ο δακτύλιος πολυωνύμων με συντελεστές από το σώμα $\mathbb{F}$. Ένα πολυώνυμο $\phi(x) \in \mathbb{F}[x]$, ως γνωστόν, είναι της μορφής $\phi(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ με τα $a_i \in \mathbb{F}$. Έστω k ο μεγαλύτερος

δείκτης (αν υπάρχει) έτσι ώστε ο αντίστοιχος συντλεστής a_k να είναι μη μηδενικός. Ο k ονομάζεται **βαθμός** του πολυωνύμου και συμβολίζεται $deg(\phi(x)$, ο a_k ονομάζεται **μεγιστοβάθμιος** συντελεστής. Αν ο μεγιστοβάθμιος συντελεστής σε ένα πολυώνυμο είναι το 1, τότε το πολυώνυμο ονομάζεται ***μονικό***. Για παράδειγμα, αν $\phi(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots a_1 x + a_0$, τότε το πολυώνυμο $a_n^{-1}\phi(x)$ προφανώς είναι μονικό. Το πολυώνυμο, του οποίου όλοι οι συντελεστές είναι μηδενικοί, ονομάζεται το **μηδενικό** πολυώνυμο, το συμβολίζουμε με **0** (ή απλά 0) και **δεν** του προσάπτουμε βαθμό.
Προφανώς τα πολυώνυμα μηδενικού βαθμού είναι τα μη μηδενικά στοιχεία του σώματος $\mathbb{F}$, τα **σταθερά** πολυώνυμα.

Για το βαθμό του αθροίσματος και του γινομένου δύο πολυωνύμων ισχύει η ακολουθη πρόταση, της οποίας η απόδειξη είναι άμεση.

Πρόταση Α΄.2.1. *Έστω $\phi(x)$ και $\theta(x)$ μη μηδενικά πολυώνυμα, τότε ισχύει:*

1. *Είτε $\phi(x) + \theta(x) = \mathbf{0}$ είτε $deg(\,\phi(x) + \theta(x)\,) \leq \max(\,deg\phi(x),\ deg\theta(x)\,)$. Η ανισότητα στην προηγούμενη σχέση είναι γνήσια μόνο στην περίπτωση που τα δύο πολυώνυμα έχουν τον ίδιο βαθμό και αντίθετους μεγιστοβάθμιους συντελεστές*
2. *$deg(\,\phi(x)\cdot\theta(x)\,) = deg\phi(x) + deg\theta(x)$.*

Α΄.2.1 Διαιρετότητα πολυωνύμων

Στον δακτύλιο $\mathbb{F}[x]$ μπορούμε να ορίσουμε μια διαίρεση πολυωνύμων ανάλογη με την γνωστή διαίρεση ακεραίων αριθμών.

Θεώρημα Α΄.2.2. Αλγόριθμος της διαίρεσης πολυωνύμων
Έστω $\alpha(x),\ \beta(x) \in \mathbb{F}$ με το $\beta(x)$ να μην είναι το μηδενικό πολυώνυμο. Τότε υπάρχουν μοναδικά $\pi(x),\ \upsilon(x) \in \mathbb{F}$ τέτοια ώστε
$\alpha(x) = \pi(x)\cdot\beta(x) + \upsilon(x)$ **και**
ή $\upsilon(x) = 0$ ή $deg(\upsilon(x)) < deg(\beta(x)$.

Το $\alpha(x)$ ονομάζεται διαιρεταίος το $\beta(x)$ ονομαζεται διαιρέτης και τα $\pi(x),\ \upsilon(x)$ πηλίκο και υπόλοιπο αντίστοιχα.

Απόδειξη. Έστω $\mathcal{A} = \{\,\alpha(x) - \beta(x)\,\tau(x), \acute{o}\pi o\upsilon\tau(x) \in \mathbb{F}[x]\,\}$. Αν το μηδενικό πολυώνυμο ανήκει στο σύνολο $\mathcal{A}$, τότε υπάρχει $\pi(x) \in \mathbb{F}[x]$ έτσι ώστε $\alpha(x) - \beta(x)\,\pi(x) = \mathbf{0}$, οπότε τα $\pi(x)$ και $\upsilon(x) = \mathbf{0}$ πληρούν τις υποθέσεις του Θεωρήματος.

Υποθέτουμε ότι το μηδενικό πολυώνυμο δεν ανήκει στο σύνολο $\mathcal{A}$. Έστω $\upsilon(x) = \alpha(x) - \beta(x)\,\pi(x)$ ένα στοιχείο του συνόλου $\mathcal{A}$ με τον μικρότερο δυνατό βαθμό. Τότε προφανώς $\alpha(x) = \beta(x)\,\pi(x) + \upsilon(x)$.

Θα δείξουμε ότι $deg(\,\upsilon(x)\,) < deg(\,\beta(x)\,)$. Πράγματι, υποθέτουμε ότι $\upsilon(x) = \alpha(x) - \beta(x)\,\pi(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots a_1 x + a_0$, $\beta(x) = bx^m + bx^{m-1} + \cdots + b_1 x + b_0$ και $deg(\,\upsilon(x)\,) = n \geq m = deg(\,\beta(x)\,)$. Τότε τα πολυώνυμα $\upsilon(x)$ και $(a_n b_m^{-1})x^{n-m}\cdot\beta(x)$ είναι του ιδίου βαθμού και έχουν αντιθετους συντελεστές, επομένως το πολυώνυμο $\upsilon(x)-(a_n b_m^{-1})x^{n-m}\cdot\beta(x)$, έχει βαθμό (γνήσια) μικρότερο απο το βαθμό του $\upsilon(x)$ και επιπλέον $\upsilon(x) - (a_n b_m^{-1})x^{n-m}\cdot\beta(x) = \alpha(x) - \beta(x)\,\pi(x) - (a_n b_m^{-1})x^{n-m}\cdot\beta(x) = \alpha(x) - (\,\pi(x) + (a_n b_m^{-1})x^{n-m}\,)\cdot\beta(x) \in \mathcal{A}$. Τούτο είναι άτοπο από την εκλογή του πολυωνύμου $\upsilon(x)$ ως πολυώνυμο με τον μικρότερο βαθμό από όλα τα πολυώνυμα που ανήκουν στο σύνολο $\mathcal{A}$. Επομένως $deg(\,\upsilon(x)\,) < deg(\,\beta(x)\,)$.

Τα πολυώνυμα $\pi(x)$ και $\upsilon(x)$ με την ιδιότητα $\alpha(x) = \beta(x)\cdot\pi(x) + \upsilon(x)$ και $deg(\,\upsilon\,) < deg(\,\beta(x)\,)$ είναι μοναδικά. Πραγματι, υποθέτουμε ότι εκτός από τα $\pi(x)$ και $\upsilon(x)$ υπάρχουν και τα πολυώνυμα $\pi'(x)$ και $\upsilon'(x)$ τέτοια ώστε $\alpha(x) = \beta(x)\cdot\pi'(x) + \upsilon'(x)$ και $deg(\,\upsilon'(x)\,) < deg(\,\beta(x)\,)$. Τότε αφαιρώντας κατά μέλη τις σχέσεις $\alpha(x) = \beta(x)\cdot\pi(x)+\upsilon(x)$ και $\alpha(x) = \beta(x)\cdot\pi'(x)+\upsilon'(x)$ έχουμε $\beta(x)\cdot(\,\pi(x) - \pi'(x)\,) = \upsilon(x) - \upsilon'(x)$, αν $\upsilon(x) - \upsilon'(x) \neq \mathbf{0}$, τότε και $\pi(x)-\pi'(x) \neq \mathbf{0}$, οπότε από την Πρόταση Α΄.2.1 έχουμε ότι $deg(\,\upsilon(x)-\upsilon'(x)\,) \geq deg(\,\beta(x)\,)$. Τούτο είναι άτοπο, αφού $deg(\,\upsilon(x) - \upsilon'(x)\,) \leq \max(\,deg(\,\upsilon(x)\,),\, deg(\,\upsilon'(x)\,)\,) < deg(\,\beta(x)\,)$. Άρα $\upsilon(x) = \upsilon'(x)$ και $\pi(x) = \pi'(x)$.

□

Παρατηρήσεις Α΄.2.3. 1. Στο προηγούμενο Θεώρημα, αν $\alpha(x) = \mathbf{0}$ ή $deg(\,\alpha(x)\,) < deg(\,\beta(x)\,)$, τότε προφανώς $\pi(x) = \mathbf{0}$ και $\upsilon(x) = \alpha(x)$.

2. Το προηγούμενο Θεώρημα (φαινομενικά) δεν μας δίνει ένα τρόπο υπολογισμού του πηλίκου και του υπολοίπου της διαίρεσης ενός πολυωνύμου δι' ενός άλλου πολυωνύμου. Αν όμως παρατηρήσουμε καλύτερα την απόδειξη, θα ("αναγνωρίσουμε") τη γνωστή σε όλους μας μέθοδο διαίρεσης πολυωνύμων.

Θα λέμε ότι το πολυώνυμο $\beta(x)$ διαιρεί το πολυώνυμο $\alpha(x)$ (και θα συμβολίζουμε $\beta(x)\,|\,\alpha(x)$), αν το υπόλοιπο $\upsilon(x)$, στη διαίρεση του $\alpha(x)$ με το $\beta(x)$, είναι το μηδενικό πολυώνυμο. Ισοδύναμα λέμε ότι το $\alpha(x)$ διαιρείται (ή είναι πολλαπλάσιο του) από το $\beta(x)$.

Ας δούμε μερικές άμεσες συνέπειες των προηγουμένων, τις οποίες θα χρησιμοποιούμε συχνά στα επόμενα χωρίς ιδιαίτερη αναφορά.

1. Το μηδενικό πολυώνυμο διαιρείται από κάθε άλλο πολυώνυμο. Πράγματι, για κάθε $\phi(x) \in \mathbb{F}[x]$ ως γνωστόν ισχύει $\phi(x)\,\mathbf{0} = \mathbf{0}$.
Οπότε το μηδενικό πολυώνυμο $\mathbf{0}$ διαιρεί μόνο το μηδενικό πολυώνυμο. Επομένως στα επόμενα, όταν γράφουμε $\phi(x)\,|\,\theta(x)$ θα εννοούμε (σιωπηλά) ότι $\phi(x) \neq \mathbf{0}$.

2. Υποθέτουμε ότι $\phi(x)\,|\,\theta(x)$, με $\phi(x) \neq \mathbf{0}$. Τότε υπάρχει μοναδικό $\pi(x) \in \mathbb{F}[x]$ τέτοιο ώστε $\theta(x) = \phi(x)\,\pi(x)$. Πράγματι αν υπήρχε και ένα άλλο $\pi'(x) \in \mathbb{F}[x]$ με $\theta(x) = \phi(x)\,\pi'(x)$, τότε θα είχαμε $\theta(x) = \phi(x)\,\pi(x) = \phi(x)\,\pi'(x)$. Δηλαδή $\phi(x)\,(\,\pi(x) - \pi'(x)\,) = \mathbf{0}$ και επειδή το $\phi(x)$ δεν είναι το μηδενικό πολυώνυμο έχουμε $\pi(x) - \pi'(x) = \mathbf{0}$, άρα $\pi(x) = \pi'(x)$.

3. Υποθέτουμε ότι $\phi(x)\,|\,\theta(x)$, τότε $deg(\,\phi(x)\,) \leq deg(\,\theta(x)\,)$, οπότε αν $\phi(x)\,|\,\theta(x)$ και $\theta(x)\,|\,\phi(x)$, τότε $deg(\,\phi(x)\,) = deg(\,\theta(x)\,)$.

4. Κάθε (μη μηδενικό) σταθερό πολυώνυμο c διαιρεί κάθε άλλο πολυώνυμο. Πράγματι, για κάθε $\pi(x) \in \mathbb{F}[x]$ έχουμε $\phi(x) = c \cdot (\,c^{-1} \cdot \phi(x)\,)$

5. Αν $\phi(x)\,|\,\theta(x)$, τότε για κάθε $0 \neq c \in \mathbb{F}[x]$ έχουμε ότι $c \cdot \phi(x)\,|\,\theta(x)$. Άρα αν $\phi(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots a_1 x + a_0$, τότε το μονικό πολυώνυμο $a_n^{-1} \cdot \phi(x)$ διαιρεί το $\theta(x)$

6. Υποθέτουμε ότι το πολυώνυμο $\phi(x)$ δαιρεί το πολυώνυμο $\theta(x)$ και ότι το πολυώνυμο $\theta(x)$ διαιρεί το πολυώνυμο $\sigma(x)$, τότε προφανώς το $\phi(x)$ διαιρεί το $\sigma(x)$.

7. Υποθέτουμε ότι το πολυώνυμο $\phi(x)$ διαιρεί τα πολυώνυμα $\theta_1(x)$ και $\theta_2(x)$, τότε (γιατί;) το $\phi(x)$ διαιρεί το πολυώνυμο $\alpha(x) \cdot \theta_1(x) + \beta(x) \cdot \theta_2(x)$, για όλα τα πολυώνυμα $\alpha(x),\ \beta(x) \in \mathbb{F}[x]$.

Πρόταση Α΄.2.4. *Ο δακτύλιος των πολυωνύμων $\mathbb{F}[x]$ είναι περιοχή κυρίων ιδεωδών.*

Απόδειξη. Έστω I ένα ιδεώδες του $\mathbb{F}[x]$. Αν το I είναι το μηδενικό ιδεώδες, τότε αυτό προφανώς είναι κύριο. Υποθέτουμε ότι $\mathrm{I} \neq \{\,0\,\}$. Επιλέγουμε ένα $p(x) \in \mathrm{I}$ ελαχίστου βαθμού. Τότε το $p(x)$ διαιρεί κάθε στοιχείο του I. Πράγματι, έστω $\alpha(x) \in \mathrm{I}$, από την ταυτότητα της διαίρεσης έχουμε ότι υπάρχουν $\pi(x), \upsilon(x) \in \mathbb{F}[x]$ τέτοια ώστε $\alpha(x) = p(x) \cdot \pi(x) + \upsilon(x)$ με ή $\upsilon(x) = \mathbf{0}$ ή $deg(\upsilon(x)) < deg(p(x)$. Αλλά $\upsilon(x) = \alpha(x) - p(x) \cdot \pi(x) \in \mathrm{I}$ (γιατί;) Επομένως, από τον τρόπο εκλογής του $p(x)$, έχουμε ότι αναγκαστικά $\upsilon(x) = \mathbf{0}$. Δηλαδή $\mathrm{I} = \{\,r(x) \cdot p(x) \mid r(x) \in \mathbb{F}[x]\,\} = \langle\,p(x)\,\rangle$.

□

Παρατήρηση Α΄.2.5. Επειδή ισχύει $\langle\,p(x)\,\rangle = \langle\,ap(x)\,\rangle$ για κάθε μη μηδενικό $a \in \mathbb{F}[x]$ (γιατί ισχύει;) μπορούμε να αναδιατυπώσουμε την προηγούμενη πρόταση ως εξής: "Για κάθε μη μηδενικό ιδεώδες I του δακτυλίου $\mathbb{F}[x]$ υπάρχει μοναδικό μονικό πολυώνυμο $q(x)$ έτσι ώστε $\mathrm{I} = \langle\,q(x)\,\rangle$ ".

Ένα μη σταθερό πολυώνυμο $p(x) \in \mathbb{F}$ θα λέγεται **ανάγωγο** επί του $\mathbb{F}$ αν από τη σχέση $p(x) = \sigma(x) \cdot \tau(x)$, έπεται ότι ένα από τα $\sigma(x)$, $\tau(x)$ είναι σταθερό πολυώνυμο.

Από τον ορισμό του αναγώγου πολυωνύμου έπεται ότι όλα τα πολυώνυμα με βαθμό ένα είναι ανάγωγα. Το να αποφανθούμε όμως αν ένα πολυώνυμο με βαθμό μεγαλύτερο του ένα είναι ανάγωγο δεν είναι καθόλου εύκολο και εξαρτάται από το σώμα $\mathbb{F}$ των συντελεστών. Για παράδειγμα το πολυώνυμο x^2-3 είναι ανάγωγο επί του σώματος των ρητών αριθμών $\mathbb{Q}$, αλλά **δεν** είναι ανάγωγο επί του σώματος των πραγματικών αριθμών, αφού $x^2-2=(x-\sqrt{3})(x+\sqrt{3})$.

Α΄.2.2 Μέγιστος Κοινός Διαιρέτης Πολυωνύμων

Πρίν δώσουμε τον ορισμό του μέγιστου κοινού διαιρέτη πολυωνύμων, θα θέλαμε να παρατηρήσουμε ότι, αν $\phi(x),\ \theta(x)\in\mathbb{F}[x]$, τότε, όπως έχουμε επισημάνει, κάθε σταθερό (μη μηδενικό) πολυώνυμο c διαιρεί και τα δύο πολυώνυμα. Δηλαδή για τα πολυώνυμα αυτά υπάρχουν *κοινοί διιρέτες*. Επομένως έπεται ότι υπάρχουν κοινοί διαιρέτες δύο πολυωνύμων οι οποίοι είναι μονικά πολυώνυμα.

Ορισμός Α΄.2.6. *Έστω $\phi(x),\ \theta(x)\in\mathbb{F}[x]$ όχι και τα δύο μηδενικά πολυώνυμα, ένα πολυώνυμο $d(x)\in\mathbb{F}[x]$ θα λέγεται* ***μέγιστος κοινός διαιρέτης*** *των $\phi(x)$ και $\theta(x)$ και θα συμβολίζεται $d(x)=$ μ.κ.δ.$(\phi(x),\ \theta(x))$ ή απλά $d(x)=(\phi(x),\ \theta(x))$ αν:*

(i) $d(x)|\,\phi(x)$ και $d(x)|\,\theta(x)$. Δηλαδή το πολυώνυμο $d(x)$ είναι κοινός διαιρέτης των $\phi(x)$ και $\theta(x)$.

(ii) Το $d(x)$ είναι μονικό πολυώνυμο.

(iii) Αν $\delta(x)\in\mathbb{F}[x]$ με $\delta(x)|\,\phi(x)$ και $\delta(x)|\,\theta(x)$, τότε $\delta(x)|\,d(x)$. Δηλαδή κάθε κοινός διαιρέτης των $\phi(x)$ και $\theta(x)$ είναι διαιρέτης του $d(x)$.

Ο ορισμός δεν εξασφαλίζει την υπάρξη ενός μ.κ.δ. δύο πολυωνύμων εκ των οποίων τουλάχιστον το ένα είναι μη μηδενικό.

Μπορούμε όμως να δούμε εύκολα ότι αν υπάρχει μ.κ.δ. των $\phi(x)$ και $\theta(x)$, τότε αυτός είναι μοναδικός. Πράγματι υποθέτουμε ότι υπάρχουν δύο πολυώνυμα $d_1(x)$ και $d_2(x)$ με τις ιδιότητες του ορισμού. Τότε από τις (i) και (iii) του ορισμού έχουμε ότι $d_1(x)|\,d_2(x)$ και $d_2(x)|\,d_1(x)$. Δηλαδή υπάρχει $c\in\mathbb{F}[x]$ τέτοιο ώστε $d_1(x)=c\,d_2(x)$. Αλλά τα $d_1(x),\ d_2(x)$ είναι μονικά. Άρα $d_1(x)=d_2(x)$.

Πριν αποδείξουμε ότι ο μ.κ.δ. δύο πολυωνύμων υπάρχει επισημαίνουμε ότι αν και τα δύο πολυώνυμα είναι μηδενικά πολυώνυμα, τότε ο μ.κ.δ. δεν ορίζεται, αφού η (iii) στον ορισμό δεν ικανοποιείται (γιατί;).

Θα αποδείξουμε τώρα ένα Θεώρημα το οποίο όχι μόνο μας εξασφαλίζει την ύπαρξη του μ.κ.δ. δύο πολυωνύμων, αλλά μας δίνει και μία έκφραση του ως (γραμμικό) συνδυασμό των δύο πολυωνύμων.

Θεώρημα Α΄.2.7. *Έστω $\phi(x),\ \theta(x)\in\mathbb{F}[x]$ όχι και τα δύο μηδενικά πολυώνυμα, τότε υπάρχει ο (μοναδικός) μ.κ.δ. των $\phi(x)$ και $\theta(x)$, επιπλέον υπάρχουν $\alpha(x),\ \beta(x)\in\mathbb{F}[x]$ τέτοια ώστε μ.κ.δ. $(\phi(x),\theta(x))=\alpha(x)\cdot\phi(x)+\beta(x)\cdot\theta(x)$*

Απόδειξη. Έστω $\mathcal{U} = \{\, \lambda(x)\cdot\phi(x)+\kappa(x)\cdot\theta(x) \mid \lambda(x),\, \kappa(x) \in \mathbb{F}[x] \,\}$. Παρατηρούμε ότι στο σύνολο $\mathcal{U}$ ανήκουν τα πολυώνυμα $\phi(x)$ και $\theta(x)$ (γιατί ;). Επίσης στο σύνολο $\mathcal{U}$ ανήκουν μονικά πολυώνυμα. Πράγματι αν $\eta(x) = \lambda(x)\cdot\phi(x) + \kappa(x)\cdot\theta(x)$ είναι ένα (μη μηδενικό) στοιχείο του $\mathcal{U}$ με συντελεστή του μεγιστοβαθμίου όρου c, τότε το πολυώνυμο $c^{-1}\eta(x) = (c^{-1}\lambda(x))\cdot\phi(x) + (c^{-1}\kappa(x))\cdot\theta(x)$ είναι μονικό και ανήκει στο σύνολο $\mathcal{U}$.

Από τις προηγούμενες παρατηρήσεις έπεται ότι μπορούμε να επιλέξουμε ένα στοιχείο $d(x) = \alpha(x)\cdot\phi(x)+\beta(x)\cdot\theta(x)$ του $\mathcal{U}$, το οποίο να είναι μονικό και να έχει τον μικρότερο βαθμό από όλα τα (μη μηδενικά) στοιχεία του $\mathcal{U}$.

Το $d(x)$ είναι μονικό, άρα πληροί τη συνθήκη (ii) του ορισμού.

Έστω $\delta(x) \in \mathbb{F}[x]$ με $\delta(x)|\,\phi(x)$ και $\delta(x)|\,\theta(x)$, τότε προφανώς το $\delta(x)|\,d(x)$. Δηλαδή κάθε κοινός διαιρέτης των $\phi(x)$ και $\theta(x)$ είναι διαιρέτης του $d(x)$. Άρα το $d(x)$ πληροί τη συνθήκη (iii) του ορισμού.

Απομένει να αποδείξουμε τη συνθήκη (i).

Έστω $\tau(x) = \lambda(x)\cdot\phi(x) + \kappa(x)\cdot\theta(x)$ ένα στοιχείο του συνόλου $\mathcal{U}$, θα δείξουμε ότι $d(x)|\,\tau(x)$.

Από τον αλγόριθμο διαίρεσης πολυωνύμων υπάρχουν μοναδικά $\pi(x),\, \upsilon(x) \in \mathbb{F}[x]$ τέτοια ώστε $\tau(x) = \pi(x)\,d(x) + \upsilon(x)$ με $\upsilon(x) = \mathbf{0}$ ή $deg(\,\upsilon(x)\,) < deg(\,d(x)\,)$. Επομένως έχουμε $\upsilon(x) = \tau(x) - \pi(x)\,d(x) = \lambda(x)\cdot\phi(x)+\kappa(x)\cdot\theta(x)-\pi(x)\cdot(\,\alpha(x)\cdot\phi(x)+\beta(x)\cdot\theta(x)\,) = (\,\lambda(x)-\pi(x)\,\alpha(x)\,)\cdot\phi(x)+(\,\kappa(x)-\pi(x)\,\beta(x)\,)\cdot\theta(x) \in \mathcal{U}$. Υποθέτουμε ότι το $\upsilon(x)$ δεν είναι το μηδενικό πολυώνυμο, αν c είναι ο συντελεστής του μεγιστοβαθμίου όρου του, τότε το πολυώνυμο $c^{-1}\upsilon(x)$ είναι μονικό, ανήκει στο $\mathcal{U}$ και έχει βαθμό ίσο με τον βαθμό του $\upsilon(x)$, ο οποίος είναι (γνήσια) μικρότερος από το βαθμό του $d(x)$. Αυτό είναι άτοπο από την επιλογή του πολυωνύμου $d(x)$. Αρα $\upsilon(x) = \mathbf{0}$. Δηλαδή το $d(x)$ είναι κοινός διαιρέτης όλων των στοιχείων του συνόλου $\mathcal{U}$, άρα και των $\phi(x)$ και $\theta(x)$.

□

Παρατηρήσεις Α΄.2.8. 1. Όπως προκύπτει από τον ορισμό και προηγούμενες παρατηρήσεις ο μ.κ.δ. δύο πολυωνύμων έχει το μεγαλύτερο βαθμό από όλους τους κοινούς διαιρέτες των δύο πολυωνύμων.

2. Έστω $\phi(x)$ και $\theta(x)$ δύο πολυώνυμα με το $\phi(x)|\,\theta(x)$. Τότε προφανώς μ.κ.δ.$(\,\phi(x),\, \theta(x)\,) = c^{-1}\phi(x)$, όπου c είναι ο συντελεστής του μεγιστοβαθμίου όρου του $\phi(x)$.

3. Έστω $\phi(x)$ και $\theta(x)$ δύο πολυώνυμα και c_1, c_2 δύο μη μηδενικά στοιχεία του συνόλου F. Τότε προφανώς μ.κ.δ. $(\,\phi(x),\, \theta(x)\,)$ = μ.κ.δ. $(\,c_1\,\phi(x),\, c_2\,\theta(x)\,)$ (γιατί ;). Επομένως στην αναζήτηση του μέγιστου κοι-

νού διαιρέτη δύο πολυωνύμων μπορούμε να "περιορισθούμε " σε μονικά πολυώνυμα.

Το προηγούμενο Θεώρημα δεν μας δίνει ένα τρόπο υπολογισμού του μ.κ.δ. δύο πολυωνύμων $\phi(x)$ και $\theta(x)$, πολύ δε περισσότερο πώς μπορούμε να υπολογίσουμε πολυώνυμα συντελεστές $\alpha(x)$ και $\beta(x)$ στην έκφραση μ.κ.δ. $(\,\phi(x),\,\theta(x)\,) = \alpha(x)\cdot\phi(x)+\beta(x)\cdot\theta(x)$.

Η επόμενη πρόταση είναι πολύ σημαντική και αποτελεί το κύριο βήμα τον υπολογισμό του μέγιστου κοινού διαιρέτη δύο πολυωνύμων.

Πρόταση Α΄.2.9. *Έστω $\phi(x)$ και $\theta(x)$ μη μηδενικά πολυώνυμα, αν $\upsilon(x)$ είναι το υπόλοιπο της διαίρεσης του $\theta(x)$ δια του $\phi(x)$, τότε μ.κ.δ.$(\,\theta(x),\ \phi(x)\,)$ = μ.κ.δ. $(\,\upsilon(x),\ \phi(x)\,)$.*

Απόδειξη. Από την ταυτότητα της διαίρεσης έχουμε ότι υπάρχει(μοναδικό) $pi(x)\in\mathbb{F}[x]$ τέτοιο ώστε $\theta(x) = \pi(x)\,\phi(x)+\upsilon(x)$. Έστω
$d_1(x)$ =μ.κ.δ.$(\,\theta(x),\ \phi(x)\,)$ και $d_2(x)$ =μ.κ.δ. $(\,\upsilon(x),\ \phi(x)\,)$. Τότε προφανώς το $d_1(x)$ είναι ένας κοινός διαιρέτης των $\upsilon(x) = \theta(x)-\pi(x)\,\phi(x)$ και $\phi(x)$, άρα $d_1(x)|d_2(x)$. Επίσης το πολυώνυμο $d_2(x)$ είναι ένας κοινός διαιρέτης των $\phi(x)$ και $\theta(x) = \pi(x)\,\phi(x)+\upsilon(x)$, άρα $d_2(x)|d_1(x)$. Όποτε, επειδή τα $d_1(x)$ και $d_2(x)$ είναι μονικά έχουμε ότι $d_1(x) = d_2(x)$.

□

Εφαρμόζοντας διαδοχικά την προηγούμενη πρόταση και το γεγονός ότι "Το υπόλοιπο της διαίρεσης δύο πολυωνύμων είναι ή το μηδενικό ή έχει βαθμό γνήσια μικρότερο από το βαθμό του διαιρέτη", σε πεπερασμένα βήματα θα φτάσουμε σε μηδενικό υπόλοιπο. Το προτελευταίο (μονικό) υπόλοιπο αυτής της διαδικασίας είναι ο ζητούμενος μ.κ.δ..

Πράγματι, έστω $\theta(x),\ \phi(x)\in\mathbb{F}[x]$ με το $\phi(x)$ μη μηδενικό, τότε από τον αλγόριθμο της διαίρεσης διαδοχικά έχουμε

$\theta(x) = \pi_1(x)\,\phi(x)+\upsilon_1(x), \quad deg(\,\upsilon_1(x)\,) < deg(\,\phi(x)\,)$
$\phi(x) = \pi_2(x)\,\upsilon_1(x)+\upsilon_2(x), \quad deg(\,\upsilon_2(x)\,) < deg(\,\upsilon_1(x)\,)$
$\upsilon_1(x) = \pi_3(x)\,\upsilon_2(x)+\upsilon_3(x), \quad deg(\,\upsilon_3(x)\,) < deg(\,\upsilon_2(x)\,)$
$\upsilon_2(x) = \pi_4(x)\,\upsilon_3(x)+\upsilon_4(x), \quad deg(\,\upsilon_4(x)\,) < deg(\,\upsilon_3(x)\,)$
....
$\upsilon_{n-2}(x) = \pi_n(x)\,\upsilon_{n-1}(x)+\upsilon_n(x), \quad deg(\,\upsilon_{n-1}(x)\,) < deg(\,\upsilon_n(x)\,)$
$\upsilon_{n-1}(x) = \pi_{n+1}(x)\,\upsilon_n(x)+\mathbf{0}$.

Μετά από n βήματα (ο αριθμός των οποίων δεν ξεπερνά τον βαθμό του $\phi(x)$) το τελευταίο υπόλοιπο $\upsilon_{n+1}(x)$ είναι το μηδενικό πολυώνυμο, αφού
$deg(\,\phi(x)\,) > deg(\,\upsilon_1(x)\,) > deg(\,\upsilon_2(x)\,) > deg(\,\upsilon_3(x)\,) > \cdots$.

Επομένως έχουμε

μ.κ.δ.($\theta(x)$, $\phi(x)$) =μ.κ.δ.($\phi(x)$, $\upsilon_1(x)$) =μ.κ.δ.($\upsilon_1(x)$, $\upsilon_2(x)$) $= \cdots =$ μ.κ.δ.($\upsilon_n(x)$, $\mathbf{0}$). Οπότε το αντίστοιχο μονικό πολυώνυμο του $\upsilon_n(x)$ είναι ο ζητούμενος μέγιστος κοινός διαιρέτης.

Για τον υπολογισμό των πολυωνύμων συντελεστών $\alpha(x)$ και $\beta(x)$ στην έκφραση μ.κ.δ. ($\phi(x)$, $\theta(x)$) $= \alpha(x)\cdot\phi(x)+\beta(x)\cdot\theta(x)$. Εφαρμόζουμε αντίστροφη πορεία, ξεκινώντας από την προτελευταία σχέση έχουμε

$\upsilon_n(x) = \upsilon_{n-2}(x) - \pi_n(x)\,\upsilon_{n-1}(x)$.

Αλλά $\upsilon_{n-1}(x) = \upsilon_{n-3}(x) - \pi_{n-1}(x)\,\upsilon_{n-2}(x)$ και $\upsilon_{n-2}(x) = \upsilon_{n-4}(x) - \pi_{n-2}(x)\,\upsilon_{n-3}(x)$, οπότε αντικαθιστώντας στην προηγούμενη σχέση έχουμε μια παράσταση της μορφής

$\upsilon_n(x) = \beta_{n-3}(x)\,\upsilon_{n-4}(x) + \alpha_{n-2}(x)\,\upsilon_{n-3}(x)$. Συνεχίζοντας με την ίδια διαδικασία καταλήγουμε σε μια παράσταση της μορφής

$\upsilon_n(x) = \beta_2(x)\upsilon_1(x)+\alpha_3(x)\upsilon_2(x)$ και τελικά $\upsilon_n(x) = \beta_1(x)\theta(x)+\alpha_2(x)\phi(x)$.

Έστω r ο μεγιστοβάθμιος συντελεστής του $\upsilon_n(x)$, τότε προφανώς τα ζητούμενα πολυώνυμα συντελεστές είναι $\alpha(x) = r^{-1}\alpha_2(x)$ και $\beta(x) = r^{-1}\beta_1(x)$.

Παρατήρηση Μπορούμε να ορίσουμε τον μέγιστο κοινό διαιρέτη περισσοτέρων, από δύο, πολυωνύμων.

Έστω $\phi_i(x) \in \mathbb{F}[x]$, $i = 1, 2, \ldots, n$ όχι όλα μηδενικά πολυώνυμα, ένα πολυώνυμο $d(x) \in \mathbb{F}[x]$ θα λέγεται ***μέγιστος κοινός διαιρέτης*** των $\phi_i(x)$ και θα συμβολίζεται $d(x) =$ μ.κ.δ.($\phi_1(x)$, $\phi_2(x)$, $\ldots$, $\phi_n(x)$) ή απλά
$d(x) = (\,\phi_1(x), \phi_2(x), \ldots, \phi_n(x)\,)$ αν:

(ι) $d(x)|\,\phi_i(x)$. Δηλαδή το πολυώνυμο $d(x)$ είναι κοινός διαιρέτης των $\phi_i(x)$.

(ιι) Το $d(x)$ είναι μονικό πολυώνυμο.

(ιιι) Αν $\delta(x) \in \mathbb{F}[x]$ με $\delta(x)|\,\phi_i(x)$, τότε $\delta(x)|\,d(x)$. Δηλαδή κάθε κοινός διαιρέτης των $\phi_i(x)$ είναι διαιρέτης του $d(x)$.

Η ύπαρξη, η μοναδικότητα και ο υπολογισμός του μέγιστου κοινού διαιρέτη περισσοτέρων των δύο πολυωνύμων βασίζεται στην εξής απλή παρατήρηση. Έστω $\phi(x)$, $\theta(x)$, $\sigma(x) \in \mathbb{F}[x]$, τότε υπάρχει ο μ.κ.δ.($\phi(x)$, $\theta(x)$, $\sigma(x)$) και ισχύει μ.κ.δ.($\phi(x)$, $\theta(x)$, $\sigma(x)$) =μ.κ.δ.(μ.κ.δ.($\phi(x)$, $\theta(x)$), $\sigma(x)$). Πράγματι έστω $d_1(x)$ =μ.κ.δ.($\phi(x)$, $\theta(x)$) και $d_2(x)$ =μ.κ.δ.(μ.κ.δ.($\phi(x)$, $\theta(x)$), $\sigma(x)$) = =μ.κ.δ.($d_1(x)$, $\sigma(x)$).

Έστω $d(x)$ ένας κοινός διαιρέτης των $\phi(x)$ και $\theta(x)$, άρα $d(x)|\,d_1(x)$ είναι όμως και διαιρέτης του $\sigma(x)$, επομένως $d(x)|\,d_2(x)$.

Αλλά $d_2(x)|\,d_1(x)$ και το $d_1(x)$ διαιρεί το $\phi(x)$ και το $\theta(x)$, άρα το $d_2(x)$ είναι ένας κοινός διαιρέτης των $\phi(x)$ και $\theta(x)$, επίσης το $d_2(x)|\,\sigma(x)$. Άρα το $d_2(x)$ είναι ένας κοινός διαιρέτης των $\phi(x)$, $\theta(x)$ και $\sigma(x)$, ο οποίος διαιρείται από τον (τυχαίο) κοινό διαιρέτη $d(x)$. Συνεπώς $d_2(x)$ =μ.κ.δ.($\phi(x)$, $\theta(x)$, $\sigma(x)$).

Από την προηγούμενη έκφραση του μ.κ.δ. των πολυωνύμων $\phi(x)$, $\theta(x)$, $\sigma(x)$ εύκολα προκύπτει ότι και στην περίπτωση αυτή ισχύει ένα θεώρημα ανάλογο με το

Θεώρημα Α΄.2.7 (Ως άσκηση προσπάθησε μόνος να διατυπώσεις και να αποδείξεις το αντίστοιχο αποτέλεσμα).

Δύο πολυώνυμα $\theta(x)$ και $\phi(x)$ θα λέγονται ***σχετικά πρώτα*** ή ***πρώτα μεταξύ τους*** αν μ.κ.δ. $(\theta(x),\ \phi(x)) = 1$

Θεώρημα Α΄.2.10. *Έστω* $\phi(x),\ \theta(x),\ \sigma(x) \in \mathbb{F}[x]$ *με* μ.κ.δ.$(\phi(x),\ \theta(x)) = 1$ *και* $\phi(x) | \theta(x)\sigma(x)$. *Τότε* $\phi(x) | \sigma(x)$.

Απόδειξη. Επειδή μ.κ.δ.$(\phi(x),\ \theta(x)) = 1$ υπάρχουν πολυώνυμα $\alpha(x)$ και $\beta(x)$ τέτοια ώστε μ.κ.δ. $(\phi(x), \theta(x)) = \alpha(x)\cdot\phi(x) + \beta(x)\cdot\theta(x) = 1$. Πολλαπλασιάζοντας και τα δύο μέλη της τελευταίας σχέσης με το πολυώνυμο $\sigma(x)$ έχουμε $\alpha(x)\cdot\phi(x)\cdot\sigma(x) + \beta(x)\cdot\theta(x)\cdot\sigma(x) = \sigma(x)$. Το πολυώνυμο $\phi(x)$ διαιρεί το $\beta(x)\cdot\theta(x)\cdot\sigma(x)$, από την υπόθεση, προφανώς διαιρεί και το $\alpha(x)\cdot\phi(x)\cdot\sigma(x)$, άρα διαιρεί και το άθροισμα $\alpha(x)\cdot\phi(x)\cdot\sigma(x) + \beta(x)\cdot\theta(x)\cdot\sigma(x) = \sigma(x)$.

□

Πόρισμα Α΄.2.11. *Έστω* $\phi(x),\ \theta(x),\ \sigma(x) \in \mathbb{F}[x]$ *με* μ.κ.δ.$(\phi(x),\ \theta(x)) = 1$, $\phi(x) | \sigma(x)$ *και* $\theta(x) | \sigma(x)$. *Τότε* $\phi(x)\theta(x) | \sigma(x)$

Πρόταση Α΄.2.12. *Έστω* $p(x), p_1(x), \ldots, p_n(x) \in \mathbb{F}[x]$ *ανάγωγα πολυώνυμα. Υποθέτουμε ότι το πολυώνυμο* $p(x)$ *διαιρεί το γινόμενο* $p_1(x)\cdots p_n(x)$, *τότε υπάρχει* $c \in F$ *έτσι ώστε* $p(x) = cp_i(x)$ *για κάποιο δείκτη* i.

Απόδειξη. Επειδή το πολυώνυμο $p(x)$ είναι ανάγωγο θα έχουμε είτε $p(x) | p_1(x)$ είτε μ.κ.δ.$(p(x),\ p_1(x)) = 1$ (γιατί ;). Αν $p(x) | p_1(x)$ έχει καλώς, αν μ.κ.δ.$(p(x),\ p_1(x)) = 1$, τότε από την υπόθεση και την προηγούμενη Πρόταση έχουμε ότι το πολυώνυμο $p(x)$ διαιρεί το γινόμενο $p_2(x)\cdots p_n(x)$. Οπότε πάλι είτε $p(x) | p_2(x)$ είτε μ.κ.δ.$(p(x),\ p_2(x)) = 1$. Συνεχίζοντας αυτή τη διαδικασία σε πεπερασμένα βήματα θα καταλήξουμε ότι υπάρχει $1 \le i \ge n$ έτσι ώστε $p(x) | p_i(x)$. Τα πολυώνυμα όμως $p(x)$ και $p_i(x)$ είναι ανάγωγα οπότε αναγκαστικά θα υπάρχει $c \in F$ έτσι ώστε $p(x) = cp_i(x)$.

□

Πρόταση Α΄.2.13. *Κάθε μη σταθερό πολυώνυμο* $\phi(x)$ *διαιρείται από (τουλάχιστον) ένα ανάγωγο πολυώνυμο.*

Απόδειξη. Θα εφαρμόσουμε επαγωγή στο βαθμό, έστω n, του $\phi(x)$. Αν το $\phi(x)$ είναι ανάγωγο, τότε αυτό διαιρείται από τον εαυτό του. Υποθέτουμε ότι το $\phi(x)$ δεν είναι ανάγωγο και ότι όλα τα μη σταθερά πολυώνυμα με βαθμό μικρότερο του n διαιρούνται από ένα ανάγωγο πολυώνυμο. Για το $\phi(x)$ υπάρχουν μη σταθερά πολυώνυμα $\phi_1(x)$ και $\phi_2(x)$ τέτοια ώστε $\phi(x) = \phi_1(x)\,\phi_2(x)$. Τα

$\phi_1(x)$ και $\phi_2(x)$ έχουν βαθμό μικρότερο του n και επομένως από την υπόθεση της επαγωγής κάθε ένα από αυτά διαιρείται από ένα ανάγωγο πολυώνυμο, άρα και το $\phi(x)$ διαιρείται από ένα ανάγωγο πολυώνυμο.

□

Θεώρημα Α΄.2.14. *Κάθε μη σταθερό πολυώνυμο $\phi(x) \in \mathbb{F}[x]$ γράφεται ως γινόμενο αναγώγων πολυωνύμων στο $\mathbb{F}[x]$ κατά μοναδικό τρόπο. Συγκεκριμένα υπάρχουν μοναδικά μονικά ανάγωγα πολυώνυμα $p_i(x) \in \mathbb{F}[x]$, $i = 1, 2, \ldots, n$ και μοναδικό $c \in \mathbb{F}[x]$ τέτοια ώστε $\phi(x) = c\,p_1(x)\,p_2(x)\cdots p_n(x)$.*

Απόδειξη. Θα εφαρμόσουμε επαγωγή στο βαθμό του πολυωνύμου $\phi(x)$. Αν $deg(\,\phi(x)\,) = 1$, τότε το πολυώνυμο $\phi(x)$ είναι ανάγωγο και το θεώρημα ισχύει (εδώ θεωρούμε ότι έχουμε γινόμενο με ένα ανάγωγο όρο). Υποθέτουμε ότι το θεώρημα ισχύει για όλα τα πολυώνυμα με βαθμό μικρότερου του βαθμού του $\phi(x)$. Αν το $\phi(x)$ είναι ανάγωγο, τότε πάλι το θεώρημα ισχύει. Υποθέτουμε ότι το $\phi(x)$ δεν είναι ανάγωγο. Άρα υπάρχουν πολυώνυμα $\phi_1(x)$ και $\phi_2(x)$ τέτοια ώστε $\phi(x) = \phi_1(x)\,\phi_2(x)$. Ο βαθμός των $\phi_1(x)$ και $\phi_2(x)$ είναι μικρότερος του βαθμού του $\phi(x)$, άρα το θεώρημα ισχύει για αυτά τα πολυώνυμα, όποτε και το $\phi(x)$ μπορεί να γραφεί στη μορφή $\phi(x) = c\,p_1(x)\,p_2(x)\cdots p_n(x)$ με $c \in \mathbb{F}[x]$ και τα $p_i(x)$ μονικά και ανάγωγα.

Ας υποθέσουμε τώρα ότι $\phi(x) = c_1\,p_1(x)\,p_2(x)\cdots p_n(x) =$
$= c_2\,q_1(x)\,q_2(x)\cdots q_m(x)$, όπου $c_1, c_2 \in F$ και τα πολυώνυμα
$p_1(x), p_2(x), \ldots, p_n(x), q_1(x), q_2(x), \ldots, q_m(x)$ είναι μονικά και ανάγωγα επί του F. Το πολυώνυμο $q_m(x)$ διαιρεί το γινόμενο $c_1\,p_1(x)\,p_2(x)\cdots p_n(x)$, επομένως σύμφωνα με την προηγούμενη πρόταση υπάρχει $c \in F$ έτσι ώστε $q_m(x) = c\,p_i(x)$ για κάποιο δείκτη i. Αλλά τα $q_m(x)$ και $p_i(x)$ είναι μονικά, οπότε $q_m(x) = p_i(x)$ και αλλάζοντας, εν ανάγκη, τη σειρά των παραγόντων μπορούμε να υποθέσουμε ότι $q_m(x) = p_n(x)$. Τώρα από τη σχέση $c_1\,p_1(x)\,p_2(x)\cdots p_n(x) = c_2\,q_1(x)\,q_2(x)\cdots q_m(x)$ έχουμε ότι $c_1\,p_1(x)\,p_2(x)\cdots p_{n-1}(x) =$
$= c_2\,q_1(x)\,q_2(x)\cdots q_{m-1}(x)$. Ο βαθμός όμως του πολυωνύμου
$c_1\,p_1(x)\,p_2(x)\cdots p_{n-1}(x)$ είναι μικρότερος από τον βαθμό του $\phi(x)$, επομένως από την υπόθεση της επαγωγής έχουμε ότι $c_1 = c_2$, $n-1 = m-1$ και αλλάζοντας, εν ανάγκη, την σειρά των παραγόντων $p_i(x) = q_i(x)$.

□

Παρατηρήσεις Α΄.2.15. 1. Στην προηγούμενη γραφή ενός πολυωνύμου ως γινόμενο αναγώγων μονικών πολυωνύμων οι παράγοντες $p_i(x)$ δεν είναι κατ' ανάγκη διακεκριμένοι, οπότε θα μπορούσαμε να γράψουμε το πολυώνυμο στη μορφή $\phi(x) = c_1\,p_1^{\lambda_1}(x)\,p_2^{\lambda_2}(x)\cdots p_m^{\lambda_m}(x)$, όπου τώρα τα πολυώνυμα $p_i(x)$ είναι διακεκριμένα και τα λ_i είναι θετικοί ακέραιοι αριθμοί. Η (μονα-

δική) αυτή γραφή ονομάζεται **ανάλυση του $\phi(x)$ σε γινόμενο μονικών αναγώγων πολυωνύμων**.

2. Όπως έχουμε επισημάνει έχει σημασία επί ποίου συνόλου συντελεστών εξετάζουμε αν ένα πολυώνυμο είναι ανάγωγο. Επομένως θα έχουμε και την αντίστοιχη ανάλυση ενός πολυωνύμου σε γινόμενο μονικών αναγώγων πολυωνύμων. Για παράδειγμα, το πολυώνυμο $x^4 - x^2 - 2 \in \mathbb{R}[x]$ έχει την ανάλυση $x^4 - x^2 - 2 = (x^2 - 2)(x^2 + 1)$, ενώ το ίδιο πολυώνυμο, αν θεωρηθεί ως στοιχείο του $\mathbb{C}[x]$, έχει την ανάλυση $x^4 - x^2 - 2 = (x + \sqrt{2})(x - \sqrt{2})(x - i)(x + i)$.

3. Όπως βλέπουμε, η προηγούμενη απόδειξη δεν μας δίνει έναν (αλγόριθμο) τρόπο να υπολογίζουμε τους ανάγωγους παράγοντες στην ανάλυση ένος πολυωνύμου. Το πρόβλημα του προσδιορισμού των αναγώγων παραγόντων ενός πολυωνύμου είναι αρκετά δύσκολο και είναι ανάλογο με το πρόβλημα του προσδιορισμού των πρώτων παραγόντων στους οποίους αναλύεται ένας ακέραιος αριθμός.

Α΄.2.3 Ελάχιστο κοινό πολλαπλάσιο πολυωνύμων

Πριν δώσουμε τον ορισμό του ελαχίστου κοινού πολλαπλασίου δύο πολυωνύμων θα θέλαμε να παρατηρήσουμε ότι, αν $\phi(x),\ \theta(x) \in F[x]$, τότε το πολυώνυμο $\phi(x)\,\theta(x)$ διαιρείται από τα δύο πολυώνυμα $\phi(x)$ και $\theta(x)$. Δηλαδή είναι ένα *κοινό πολλαπλάσιο* των $\phi(x)$ και $\theta(x)$. Όμως αν ένα πολυώνυμο $\sigma(x)$ με συντελεστή μεγιστοβαθμίου όρου c είναι πολλαπλάσιο ενός πολυωνύμου, έστω $\delta(x)$, τότε και το πολυώνυμο $c^{-1}\,\sigma(x)$ είναι πολλαπλάσιο του $\delta(x)$ (γιατί ;). Επομένως για τα πολυώνυμα $\phi(x)$ και $\theta(x)$ υπάρχουν μονικά κοινά πολλαπλάσια.

Ορισμός Α΄.2.16. *Έστω $\phi(x),\ \theta(x) \in F[x]$, ένα πολυώνυμο $m(x) \in F[x]$ θα λέγεται* ***ελάχιστο κοινό πολλαπλάσιο*** *των $\phi(x)$ και $\theta(x)$ και θα συμβολίζεται $m(x) = \epsilon.\kappa.\pi.(\,\phi(x),\ \theta(x)\,)$ ή απλά $m(x) = [\,\phi(x),\ \theta(x)\,]$ αν:*

(i) $\phi(x) \,|\, m(x)$ και $\theta(x) \,|\, m(x)$. Δηλαδή το πολυώνυμο $m(x)$ είναι κοινό πολλαπλάσιο των $\phi(x)$ και $\theta(x)$.

(ii) Το $m(x)$ είναι μονικό πολυώνυμο.

(iii) Αν $\mu(x) \in F[x]$ με $\phi(x) \,|\, \mu(x)$ και $\theta(x) \,|\, \mu(x)$, τότε $m(x) \,|\, \mu(x)$. Δηλαδή κάθε κοινό πολλαπλάσιο των $\phi(x)$ και $\theta(x)$ είναι πολλαπλάσιο του $m(x)$.

Ο ορισμός δεν εξασφαλίζει την υπάρξη ενός ε.κ.π. δύο πολυωνύμων.

Μπορούμε όμως να δούμε εύκολα ότι αν υπάρχει ε.κ.π. των $\phi(x)$ και $\theta(x)$, τότε αυτό είναι μοναδικό. Πράγματι υποθέτουμε ότι υπάρχουν δύο πολυώνυμα $m_1(x)$ και $m_2(x)$ με τις ιδιότητες του ορισμού. Τότε από τις (i) και (iii) του

ορισμού έχουμε ότι $m_1(x)|\, m_2(x)$ και $m_2(x)|\, m_1(x)$. Δηλαδή υπάρχει $c \in F[x]$ τέτοιο ώστε $m_1(x) = c\, m_2(x)$. Αλλά τα $m_1(x)$, $m_2(x)$ είναι μονικά. Άρα $m_1(x) = m_2(x)$.

Πριν αποδείξουμε ότι το ε.κ.π. δύο πολυωνύμων υπάρχει επισημαίνουμε ότι αν (τουλάχιστον) ένα από τα δύο πολυώνυμα είναι το μηδενικό πολυώνυμο, τότε το ε.κ.π. είναι το μοναδικό κοινό πολλαπλάσιο των δύο πολυωνύμων, δηλαδή το μηδενικό πολυώνυμο. Επομένως μπορούμε να υποθέτουμε ότι τα δύο πολυώνυμα είναι μη μηδενικά.

Πρόταση Α΄.2.17. *Έστω δύο μη μηδενικά πολυώνυμα $\phi(x),\ \theta(x) \in F[x]$. Τότε το ε.κ.π. των δύο πολυωνύμων είναι το μονικό πολυώνυμο με το μικρότερο βαθμό, το οποίο διαιρείται από το $\phi(x)$ και $\theta(x)$.*

Απόδειξη. Έστω $\mathcal{V} = \{\, \sigma(x) \in F[x] \mid \sigma(x)$ κοινό πολλαπλάσιο των $\phi(x)$και$\theta(x)\,\}$. Το σύνολο $\mathcal{V}$ περιέχει μη μηδενικά πολυώνυμα (γιατί ;). Επίσης, όπως έχουμε παρατηρήσει, το $\mathcal{V}$ περιέχει (και) μονικά πολυώνυμα. Έστω $m(x) \in \mathcal{V}$ ένα μονικό πολυώνυμο με τον μικρότερο βαθμό.

Το $m(x)$ διαιρεί κάθε πολυώνυμο που ανήκει στο σύνολο $\mathcal{V}$. Πράγματι, αν $\sigma(x)$ είναι ένα στοιχείο του συνόλου $\mathcal{V}$, τότε από τον αλγόριθμο της διαίρεσης έχουμε ότι υπάρχουν (μοναδικά) πολυώνυμα $\pi(x),\ \upsilon(x) \in F[x]$ τέτοια ώστε $\sigma(x) = \pi(x)\, m(x) + \upsilon(x)$ με $deg(\,\upsilon(x)\,) < deg(\,m(x)\,)$, εκτός εάν το πολυώνυμο $\upsilon(x)$ είναι το μηδενικό πολυώνυμο. Τα πολυώνυμα $\phi(x)$ και $\theta(x)\,\}$ διαιρούν το πολυώνυμο $\sigma(x) - \pi(x)\, m(x) = \upsilon(x)$ (γιατί ;). Δηλαδή το $\upsilon(x)$ είναι κοινό πολλαπλάσιο των $\phi(x)$ και $\theta(x)\,\}$, άρα ένα στοιχείο του συνόλου $\mathcal{V}$. Τούτο είναι άτοπο από την επιλογή του πολυωνύμου $m(x)$. Άρα $\upsilon(x) = \mathbf{0}$.

□

Παρατήρηση Α΄.2.18. Έστω δύο μη μηδενικά πολυώνυμα $\phi(x),\ \theta(x) \in F[x]$, αν υποθέσουμε ότι οι μεγιστοβάθμιοι συντελεστές των $\phi(x)$ και $\theta(x)$ είναι αντίστοιχα c και r, τότε προφανώς ε.κ.π.$(\,\phi(x),\ \theta(x)\,)$ =ε.κ.π.$(\,c^{-1}\phi(x),\ r^{-1}\theta(x)\,)$. Επομένως για την εύρεση του ε.κ.π. δύο πολυωνύμων αρκεί να περιορισθούμε σε μονικά πολυώνυμα.

Σχόλιο Για το ελάχιστο κοινό πολλαπλάσιο δύο πολυωνύμων δεν ισχύει ένα θεώρημα *ανάλογο* με το Θεώρημα Α΄.2.7. Πολύ δε περισσότερο δεν ισχύει κάτι ανάλογο με τον Ευκλείδιο Αλγόριθμο για τον υπολογισμό του ελαχίστου κοινού πολλαπλασίου δύο πολυωνύμων. Ισχύει όμως η εξής σημαντική σχέση που συνδέει τον μέγιστο κοινό διαιρέτη και το ελάχιστο κοινό πολλαπλάσιο δύο μονικών πολυωνύμων $\phi(x)$ και $\theta(x)$.

ε.κ.π.$(\,\phi(x),\ \theta(x)\,)$·μ.κ.δ.$(\,\phi(x),\ \theta(x)\,) = \phi(x) \cdot \theta(x)$.

Η απόδειξη της οποίας αφήνεται ως άσκηση .

Μπορούμε να ορίσουμε το ελάχιστο κοινό πολλαπλάσιο περισσοτέρων, από δύο, πολυωνύμων.

Έστω $\phi_i(x) \in F[x]$, $i = 1, 2, \ldots, n$ μη μηδενικά πολυώνυμα, ένα πολυώνυμο $m(x) \in F[x]$ θα λέγεται ***ελάχιστο κοινό πολλαπλάσιο*** των $\phi_i(x)$ και θα συμβολίζεται $m(x) = \text{ε.κ.π.}(\phi_1(x), \phi_2(x), \ldots, \phi_n(x))$ ή απλά
$m(x) = (\phi_1(x), \phi_2(x), \ldots, \phi_n(x))$ αν:

(ι) $\phi_i(x) | m(x)$. Δηλαδή το πολυώνυμο $m(x)$ είναι κοινό πολλαπλάσιο των $\phi_i(x)$.

(ιι) Το $m(x)$ είναι μονικό πολυώνυμο.

(ιιι) Αν $\mu(x) \in F[x]$ με $\phi_i(x) | \mu(x)$, τότε $m(x) | \mu(x)$. Δηλαδή κάθε κοινό πολλαπλάσιο των $\phi_i(x)$ είναι πολλαπλάσιο του $m(x)$.

Παρατηρήσεις Α΄.2.19. 1. Η ύπαρξη, η μοναδικότητα και ο υπολογισμός του ελαχίστου κοινού πολλαπλασίου περισσοτέρων των δύο πολυωνύμων βασίζεται στην εξής απλή παρατήρηση. Έστω $\phi(x), \theta(x), \sigma(x) \in F[x]$, τότε υπάρχει το $\text{ε.κ.π.}(\phi(x), \theta(x), \sigma(x))$ και ισχύει
$\text{ε.κ.π.}(\phi(x), \theta(x), \sigma(x)) = \text{ε.κ.π.}(\text{ε.κ.π.}(\phi(x), \theta(x)), \sigma(x))$.

Πράγματι, έστω $m_1(x) = \text{ε.κ.π.}(\phi(x), \theta(x))$ και
$m_2(x) = \text{ε.κ.π.}(\text{ε.κ.π.}(\phi(x), \theta(x)), \sigma(x)) = \text{ε.κ.π.}(d_1(x), \sigma(x))$.

Έστω $m(x)$ ένα κοινό πολλαπλάσιο των $\phi(x)$ και $\theta(x)$, άρα $m_1(x) | m(x)$ είναι όμως και πολλαπλάσιο του $\sigma(x)$, επομένως $m_2(x) | m(x)$. Αλλά $m_1(x) | m_2(x)$ και το $m_1(x)$ είναι πολλαπλάσιο των $\phi(x)$ και $\theta(x)$, άρα το $m_2(x)$ είναι ένα κοινό πολλαπλάσιο των $\phi(x)$ και $\theta(x)$, επίσης το $\sigma(x) | m_2(x)$. Άρα το $m_2(x)$ είναι ένα κοινό πολλαπλάσιο των $\phi(x)$, $\theta(x)$ και $\sigma(x)$, το οποίο διαιρεί το (τυχαίο) κοινό πολλαπλάσιο $m(x)$. Συνεπώς $m_2(x) = \text{ε.κ.π.}(\phi(x), \theta(x), \sigma(x))$.

2. Χρησιμοποιώντας την ανάλυση ενός πολυωνύμου σε γινόμενο αναγώγων πολυωνύμων μπορούμε να υπολογίσουμε τον μέγιστο κοινό διαιρέτη και το ελάχιστο κοινό πολλαπλάσιο δύο πολυωνύμων.

Έστω δύο πολυώνυμα $\phi(x)$ και $\theta(x)$ και έστω
$\phi(x) = c_1 p_1^{\lambda_1}(x) p_2^{\lambda_2}(x) \cdots p_m^{\lambda_m}(x)$ και $\theta(x) = c_2 p_1^{\nu_1}(x) p_2^{\nu_2}(x) \cdots p_m^{\nu_m}(x)$
οι αναλύσεις τους σε γινόμενο μονικών αναγώγων πολυωνύμων, όπου τα λ_i και ν_i ενδέχεται να είναι και μηδέν όταν ένας παράγοντας δεν εμφανίζεται στην αντίστοιχη ανάλυση του πολυωνύμου. Θέτουμε $\mu_i = min(\lambda_i, \nu_i)$ και $M_i = max(\lambda_i, \nu_i)$. Τότε μπορούμε να αποδείξουμε ότι
μ.κ.δ. $(\phi(x), \theta(x)) = p_1^{\mu_1}(x) p_2^{\mu_2}(x) \cdots p_m^{\mu_m}(x)$
και ε.κ.π.$(\phi(x), \theta(x)) = p_1^{M_1}(x) p_2^{M_2}(x) \cdots p_m^{M_m}(x)$.

Α΄.2.4 Ρίζες πολυωνύμων

Έστω $\mathbb{F}$ ένα σώμα και $\mathbb{E}$ μια επέκταση του $\mathbb{F}$. Αν $c \in \mathbb{E}$, ορίζουμε την απεικόνιση $\varphi_c : \mathbb{F}[x] \longrightarrow \mathbb{E}$ ως εξής: Αν $\sigma(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, τότε $\varphi_c(\sigma(x)) =: \sigma(c) = a_n x^n + a_{n-1}c^{n-1} + \cdots + a_1 c + a_0$. Δηλαδή η εικόνα του $\sigma(x)$ μέσω της φ_c είναι η τιμή του πολυωνύμου $\sigma(x)$ στη θέση c. Έστω $\sigma(x) \in \mathbb{F}$ έτσι ώστε $\sigma(c) = 0$, τότε το c θα ονομάζεται **ρίζα** του $\sigma(x)$.

Προφανώς ένα $c \in \mathbb{E}$ είναι ρίζα του $\sigma(x) \in \mathbb{F}$ αν και μόνο αν υπάρχει $\pi(x) \in \mathbb{E}$, έτσι ώστε $\sigma(x) = (x - c) \cdot \pi(x)$. (Προσοχή! το $\pi(x)$ δεν έχει κατ' ανάγκη συντελεστές από το σώμα $\mathbb{F}$).
Επομένως συμπεραίνουμε ότι ο αριθμός των ριζών ενός πολυωνύμου δεν υπερβαίνει τον βαθμό του.

Η απεικόνιση φ_c είναι ομομορφισμός δακτυλίων (ο έλεγχος είναι εύκολος). Έστω $p(x)$ ένα στοιχείο του πυρήνα της φ_c, τότε $\varphi_c(p(x)) = p(c) = 0$. Δηλαδή ο πυρήνας της φ_c αποτελείται από όλα τα πολυώνυμα του $\mathbb{F}[x]$, τα οποία έχουν ρίζα το στοιχείο c.

Αν ο πυρήνας $Ker\,\varphi_c$ είναι μη μηδενικό ιδεώδες, δηλαδή υπάρχει μη μηδενικό πολυώνυμο $p(x)$ με συντελεστές από το σώμα $\mathbb{F}$, του οποίου ρίζα είναι το στοιχείο c, τότε το c θα λέγεται **αλγεβρικό** επί του σώματος $\mathbb{F}$. Διαφορετικά ονομάζεται **υπερβατικό** επί του $\mathbb{F}$.

Αν κάθε στοιχείο μιας επέκτασης $\mathbb{E}$ του σώματος $\mathbb{F}$ είναι αλγεβρικό, τότε η $\mathbb{E}$ ονομάζεται αλγεβρική επέκταση του $\mathbb{F}$.

Πρόταση Α΄.2.20. *Μια πεπερασμένη επέκταση $\mathbb{E}$ του σώματος $\mathbb{F}$ είναι αλγεβρική.*

Απόδειξη. Η απόδειξη αφίνεται ως άσκηση. □

Πρόταση Α΄.2.21. *Έστω $c \in \mathbb{E}$ ένα στοιχείο αλγεβρικό επί του $\mathbb{F}$, τότε υπάρχει μοναδικό ανάγωγο μονικό πολυώνυμο $m_c(x) \in \mathbb{F}[x]$ με ρίζα το στοιχείο c.*

Απόδειξη. Ο πυρήνας $Ker\,\varphi_c$ είναι ίδεώδες του $\mathbb{F}[x]$. Από την Παρατήρηση Α΄.2.5 έπεται ότι υπάρχει μοναδικό μονικό πολυώνυμο $m_c(x) \in \mathbb{F}[x]$ έτσι ώστε $Ker\,\varphi_c = \langle\, m_c(x)\,\rangle$. Θα δείξουμε ότι το $m_c(x)$ είναι ανάγωγο. Υποθέτουμε ότι $m_c(x) = p_1(x) \cdot p_2(x)$ με $p_1(x), p_2(x) \in \mathbb{F}[x]$, επομένως έχουμε $m_c(c) = p_1(c) \cdot p_2(c) = 0 \in \mathbb{E}$. Δηλαδή $p_1(c) = 0$ ή $p_2(c) = 0$. Αλλά το $m_c(x)$ είναι ελαχίστου βαθμού με αυτή την ιδιότητα, άρα αναγκαστικά ένα από τα $p_i(x)$ είναι σταθερό πολυώνυμο.

□

Το πολυώνυμο $m_c(x)$ ομομάζετει **ελάχιστο** πολυώνυμο του στοιχείου c .

Πρόταση Α΄.2.22. *Έστω* $\mathbf{0} \neq r(x) \in \mathbb{F}[x]$.

i) Τα στοιχεία του δακτυλίου πηλίκων $\mathbb{F}[x]/\langle\, r(x)\,\rangle$ *είναι της μορφής* $\alpha(x) + \langle\, r(x)\,\rangle$, *όπου* $\alpha(x) = \mathbf{0}$ *ή ο βαθμός του* $\alpha(x)$ *είναι μικρότερος από τον βαθμό του* $r(x)$.

ii) Ένα $\alpha(x) + \langle\, r(x)\,\rangle \in \mathbb{F}[x]/\langle\, r(x)\,\rangle$ *είναι αντιστρέψιμο αν και μόνο αν μ.κ.δ.* $(\,\alpha(x),\ r(x)\,) = 1$.

Απόδειξη. Το πρώτο μέρος έπεται από την ταυτότητα της διαίρεσης και τον ορισμό του συμπλόκου (βλέπε σελίδα 164).

Ένα $\alpha(x) + \langle\, r(x)\,\rangle \in \mathbb{F}[x]/\langle\, r(x)\,\rangle$ είναι αντιστρέψιμο αν και μόνο αν υπάρχει $\beta(x) + \langle\, r(x)\,\rangle \in \mathbb{F}[x]/\langle\, r(x)\,\rangle$ έτσι ώστε $(\alpha(x) + \langle\, r(x)\,\rangle) \cdot (\beta(x) + \langle\, r(x)\,\rangle) = 1 + \langle\, r(x)\,\rangle$, αν και μόνο αν $\alpha(x) \cdot \beta(x) - 1 \in \langle\, r(x)\,\rangle$, αν και μόνο αν υπάρχει πολυώνυμο $s(x) \in \mathbb{F}[x]$ έτσι ώστε $\alpha(x) \cdot \beta(x) - 1 = s(x) \cdot r(x)$, αν και μόνο αν μ.κ.δ. $(\,\alpha(x),\ r(x)\,) = 1$ (βλέπε Θεώρημα Α΄.2.7). □

Πόρισμα Α΄.2.23. *Έστω* $r(x) \in \mathbb{F}[x]$, *ο δακτύλιος πηλίκων* $\mathbb{F}[x]/\langle\, r(x)\,\rangle$ *είναι σώμα αν και μόνο αν το πολυώνυμο* $r(x)$ *είναι ανάγωγο επί του* $\mathbb{F}$.

Απόδειξη. Ο $\mathbb{F}[x]/\langle\, r(x)\,\rangle$ είναι σώμα αν και μόνο αν κάθε μη μηδενικό στοιχείο του έχει αντίστροφο, αν και μόνο αν (σύμφωνα με την προηγούμενη πρόταση) κάθε μη μηδενικό πολυώνυμο με βαθμό μικρότερο από το βαθμό του $r(x)$ είναι πρώτο προς το $r(x)$, αν και μόνο αν το $r(x)$ είναι ανάγωγο. □

Έστω $\varphi_c : \mathbb{F}[x] \longrightarrow \mathbb{E}$ ο ομομορφισμός που ορίσαμε στην αρχή της παραγράφου και $\mathbb{F}[c] = \operatorname{Im}\varphi_c = \{\, \sigma(c) \mid \sigma(x) \in \mathbb{F}[x] \,\}$.

Πόρισμα Α΄.2.24. *Ο δακτύλιος εικόνα* $\mathbb{F}[c]$ *είναι σώμα αν και μόνο αν το στοιχείο* $c \in \mathbb{E}$ *είναι αλγεβρικό επί του* $\mathbb{F}$.

Απόδειξη. Η απόδειξη είναι άμεση από το $1^ο$ Θεώρημα Ισομορφισμών και τις Προτάσεις Α΄.2.21 και Α΄.2.22.

□

Σχόλιο Α΄.2.25. Προφανώς στην περίπτωση που το στοιχείο c είναι αλγεβρικό επί του $\mathbb{F}$, τότε ισχύει $\mathbb{F}[c] = \mathbb{F}(c)$ και ο βαθμός επέκτασης $[\mathbb{F}(c) : \mathbb{F}]$ είναι πεπερασμένος (γιατί;) .

Συγκεκριμμένα μπορείτε να αποδείξετε ότι ο βαθμός επέκτασης $[\mathbb{F}(c) : \mathbb{F}]$ είναι ίσος με το βαθμό του ελαχίστου πολυωνύμου του c.

Έστω $\mathbb{F}$ ενα σώμα και $\phi(x) \in \mathbb{F}[x]$, ένα πρόβλημα που αντιμετωπίζουμε, είναι κατά ποσόν υπάρχει μια επέκταση $\mathbb{F} \mid \mathbb{E}$ στην οποία το πολυώνυμο $\phi(x)$ έχει (τουλάχιστον) μια ρίζα και κατόπιν να υπολογίσουμε (αν είναι δυνατόν) μια ρίζα του $\phi(x)$.

Το πρόβλημα αυτό είναι δυϊκό του προβλήματος κατά πόσον ένα στοιχείο μιας επέκτασης του σώματος $\mathbb{F}$ είναι αλγεβρικό επί του $\mathbb{F}$.

Έστω $\phi(x) = p_1(x)p_2 \cdots p_k$ η ανάλυση του $\phi(x)$ σε γινόμενο αναγώγων πολυωνύμων. Υποθέτουμε ότι το $\phi(x)$ έχει μια ρίζα ξ σε μια επέκταση του $\mathbb{F}$, τότε το ξ είναι ρίζα ενός από τους παράγοντες $p_i(x)$. Αντίστροφα, αν ένας από τους παράγοντες $p_i(x)$ έχει μια ρίζα, τότε προφανώς και το πολυώνυμο $\phi(x)$ έχει μια ρίζα. Επομένως αρκεί να εξασφαλίσουμε ότι τα αναγώγα πολυώνυμα έχουν ρίζες.

Θεώρημα Α΄.2.26. *Για κάθε ανάγωγο πολυώνυμο $p(x) \in \mathbb{F}[x]$ υπάρχει μια επέκταση $\mathbb{F} \mid \mathbb{E}$ και ένα $c \in \mathbb{E}$ με $p(c) = 0$.*

Απόδειξη. Από το Πόρισμα Α΄.2.23, επειδή το $p(x)$ είναι ανάγωγο, έχουμε ότι ο δακτύλιος πηλίκων $\mathbb{F}[x]/\langle\, p(x)\,\rangle$ είναι σώμα.

Μέσω του φυσικού ομομορφισμού $\varphi : \mathbb{F}[x] \longrightarrow \mathbb{F}[x]/\langle\, p(x)\,\rangle$ το σώμα εμφυτεύεται στο σώμα $\mathbb{E} = \mathbb{F}[x]/\langle\, p(x)\,\rangle$ (Ο περιορισμός της φ στο $\mathbb{F}$ είναι μονομορφιρμός (γιατί;)). Έστω $c = x + \langle\, p(x)\,\rangle \in \mathbb{E}$, τότε έχουμε $p(c) = p(x + \langle\, p(x)\,\rangle) = p(x) + \langle\, p(x)\,\rangle = 0 \in \mathbb{E}$.

□

Πόρισμα Α΄.2.27. *Για κάθε πολυώνυμο $\phi(x) \in \mathbb{F}[x]$ υπάρχει μια επέκταση $\mathbb{F} \mid \mathbb{E}$ έτσι ώστε το $\phi(x)$ να αναλύεται σε γινόμενο πρωτοβαθμίων παραγόντων στο $\mathbb{E}[x]$. Δηλαδή το $\phi(x)$έχει όλες τις ρίζες του στο σώμα $\mathbb{E}$.*

Απόδειξη. Έστω n ο βαθμός του πολυωνύμου $\phi(x)$. Αν $n = 1$, τότε $\mathbb{E} = \mathbb{F}$. Υποθέτουμε ότι ο ισχυρισμός ισχύει για όλα τα πολυώνυμα με βαθμό μικρότερο του n. Από τα προηγούμενα μπορούμε να υποθέσουμε ότι το $\phi(x)$ είναι ανάγωγο (γιατί;). Από το προηγούμενο θεώρημα υπάρχει επέκταση $\mathbb{E}_0$ του $\mathbb{F}$ και $c \in \mathbb{E}_0$ έτσι ώστε $\phi(x) = (x-c)\cdot\tau(x)$ με $\tau(x) \in \mathbb{E}_0[x]$. Από την υπόθεση της επαγωγής υπάρχει επέκταση $\mathbb{E}$ του $\mathbb{E}_0$, όπου το $\tau(x)$ αναλύεται σε γινόμενο πρωτοβαθμίων παραγόντων. Άρα το $\phi(x) = (x-c)\cdot\tau(x)$ αναλύεται σε γινόμενο πρωτοβαθμίων παραγόντων στο σώμα $\mathbb{E}$. □

Ορισμός Α΄.2.28. *Έστω $\mathbb{F}$ ένα σώμα και $\phi(x) \in \mathbb{F}[x]$ μια επέκταση $\mathbb{E}$ του $\mathbb{F}$ ονομάζεται* **σώμα ριζών** *του πολυωνύμου $\phi(x)$, αν το $\phi(x)$ αναλύεται σε γινόμενο πρωτοβαθμίων παραγόντων στο $\mathbb{E}[x]$ και, αν υπάρχει σώμα $\mathbb{K}$ με $\mathbb{F} \leq \mathbb{K} \leq \mathbb{E}$ έτσι ώστε το το $\phi(x)$ να αναλύεται σε γινόμενο πρωτοβαθμίων παραγόντων στο $\mathbb{K}[x]$, τότε $\mathbb{K} = \mathbb{E}$.*

Πρόταση Α΄.2.29. *Κάθε πολυώνυμο $\phi(x) \in \mathbb{F}[x]$ έχει ένα σώμα ριζών.*

Απόδειξη. Από το Πόρισμα Α΄.2.23 έπεται ότι υπάρχει μια επέκταση $\mathbb{E}$, η οποία περιέχει όλες τις ρίζες του $\phi(x)$. Έστω $\xi_1, \xi_2, \ldots, \xi_k \in \mathbb{E}$ οι διακεκριμένες ρίζες του $\phi(x)$. Το σώμα $\mathbb{F}(\xi_1, \xi_2, \ldots, \xi_k)$ που προκύπτει με την προσάρτηση των ριζών του $\phi(x)$ στο σώμα $\mathbb{F}$ είναι προφανώς ένα σώμα ριζών του $\phi(x)$, αφού πληροί τις ιδιότητες του ορισμού. □

Από τα προηγούμενα δεν αποκλείεται ένα πολυώνυμο να έχει πολλά σώματα ριζών. Στην πραγματικότητα όμως υπάρχει μοναδικό σώμα ριζών ενός πολυωνύμου.

Θεώρημα Α΄.2.30. *Έστω $\phi(x) \in \mathbb{F}[x]$ ένα πολυώνυμο και $\mathbb{K}$, $\mathbb{L}$ δύο σώματα ριζών του $\phi(x)$. Τα $\mathbb{K}$ και $\mathbb{L}$ είναι ισόμορφα.*

Η απόδειξη του προηγουμένου Θεωρήματος, αν και σαν ιδέα δεν είναι πολύ δύσκολη, είναι μακροσκελής και παραλείπεται.
Στο εξής όμως εμείς θα ταυτίζουμε τα ισόμορφα σώματα ριζών ενός πολυωνύμου και θα λέμε το σώμα ριζών του πολυωνύμου.

Για παράδειγμα το σώμα ριζών του πολυωνύμου $x^2 - 2 \in \mathbb{Q}[x]$ είναι το $\mathbb{Q}(\sqrt{2}) \cong \mathbb{Q}[x]/\langle x^2 - 2 \rangle$.

Έστω $\phi(x) \in \mathbb{F}[x]$ ένα πολυώνυμο και c μια ρίζα του σε μια επέκταση $\mathbb{E}$, τότε το $x - c$ διαιρεί το $\phi(x)$ στο $\mathbb{E}[x]$. Έστω $(x-c)^m$ η μεγαλύτερη δύναμη του $x - c$, η οποία διαιρεί το $\phi(x)$. Δηλαδή $\phi(x) = (x-c)^m \cdot \sigma(x)$ με $\sigma(x) \in \mathbb{E}[x]$ και $\sigma(c) \neq 0$. Στην περίπτωση αυτή η ρίζα c ονομάζεται ρίζα πολλαπλότητας m.

Έστω $\phi(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{F}[x]$ και $\phi'(x) = na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + 2a_2 x + a_1 \in \mathbb{F}[x]$ η (τυπική) παράγωγος του πολυωνύμου $\phi(x)$. Είναι εύκολο να αποδείξουμε τους γνωστούς κανόνες παραγώγησης.

(i) $(\phi(x) + \theta(x))' = \phi'(x) + \theta'(x)$
(ii) $(\phi(x) \cdot \theta(x))' = \phi'(x) \cdot \theta(x) + \phi(x) \cdot \theta'(x)$.

Υποθέτουμε ότι το μη σταθερό πολυώνυμο $\phi(x)$ δεν έχει πολλαπλές ρίζες. Αν c είναι μια ρίζα του, τότε $\phi(x) = (x-c) \cdot \sigma(x)$ και $\sigma(c) \neq 0$. Οπότε έχουμε ότι $\phi'(x) = \sigma(x) + (x-c) \cdot \sigma(x)$, από την τελευταία σχέση έχουμε ότι $\phi'(c) = \sigma(c) \neq 0$. Άρα η παράγωγος $\phi'(x)$ είναι μη μηδενικό πολυώνυμο. Επομένως αποδείξαμε την εξης πρόταση.

Πρόταση Α΄.2.31. *Αν ένα μη σταθερό πολυώνυμο $\phi(x) \in \mathbb{F}[x]$ δεν έχει πολλαπλές ρίζες, τότε η παράγωγός του είναι μη μηδενικό πολυώνυμο*

Στην περίπτωση που το πολυώνυμο $\phi(x) \in \mathbb{F}[x]$ είναι ανάγωγο ισχύει και το αντίστροφο της προηγούμενης πρότασης.

Πρόταση Α΄.2.32. *Ένα ανάγωγο πολυώνυμο $\phi(x) \in \mathbb{F}[x]$ δεν έχει πολλαπλές ρίζες αν και μόνο αν η παράγωγος είναι μη μηδενικό πολυώνυμο.*

Απόδειξη. Απομένει να αποδείξουμε ότι αν $\phi'(x) \neq 0$, τότε το πολυώνυμο δεν έχει πολλαπλές ρίζες. Επειδή η παράγωγος $\phi'(x)$ δεν είναι το μηδενικό πολυώνυμο έχει βαθμό μικρότερο από τον βαθμό του $\phi(x)$, το $\phi(x)$ όμως είναι ανάγωγο άρα πρώτο προς το $\phi'(x)$. Επομένως υπάρχουν πολυώνυμα $\lambda(x)$, $\mu(x) \in \mathbb{F}[x]$ έτσι ώστε $\lambda(x)\cdot\phi(x)+\mu(x)\cdot\phi'(x) = 1$. Έστω c μια πολλαπλή ρίζα του $\phi(x)$, από την τελευταία σχέση έπεται ότι $\phi'(c) \neq 0$. Αλλά από τη σχέση $\phi(x) = (x-c)^m\cdot\sigma(x)$ με $m \geq 1$ έπεται ότι $\phi'(c) = 0$, άτοπο. □

Πόρισμα Α΄.2.33. *Ένα πολυώνυμο $\phi(x) \in \mathbb{F}[x]$ έχει πολλαπλές ρίζες αν και μόνο αν υπάρχει ανάγωγο πολυώνυμο $d(x) \in \mathbb{F}[x]$, το οποίο διαιρεί και το $\phi(x)$ και την παράγωγο $\phi'(x)$.*

Α΄.3 Πεπερασμένα Σώματα

Στην παράγραφο αυτή θα ασχοληθούμε με τα πεπερασμένα σώματα, καθώς και με ιδιότητες πολυωνύμων με συντελεστές από ένα πεπερασμένο σώμα.

Έστω $\mathbb{F}$ ένα πεπερσμένο σώμα, τότε προφανώς η χαρακτηριστική του είναι πεπερασμένη, έστω p. Επομένως το $\mathbb{F}$ είναι μια πεπερασμένη επέκταση του σώματος $\mathbb{Z}_p$. Έστω $[\mathbb{F} : \mathbb{Z}_p] = n$ ο βαθμός επέκτασης, τότε προφανώς $\mid \mathbb{F} \mid = p^n$. Δηλαδή το πλήθος των στοιχείων ενός πεπερασμένου σώματος είναι ίσο με μια δύναμη ενός πρώτου αριθμού.

Α΄.3.1 Τα πεπερασμένα σώματα ως σώματα ριζών πολυωνύμων

Λήμμα Α΄.3.1. *Έστω $\mathbb{F}$ ένα σώμα χαρακτηριστικής p. Τότε για κάθε θετικό ακέραιο n ισχύει $(a \pm b)^{p^n} = a^{p^n} \pm b^{p^n}$, για όλα τα $a, b \in \mathbb{F}$.*

Απόδειξη. Για p πρώτο και για $1 \leq k \leq p$ ο δυωνυμικός συντελεστής $\binom{p}{k}$ είναι πολλαπλάσιο του p (γιατί;). Οπότε $(a \pm b)^p = a^p \pm b^p$, με τις λεπτομέρειες να αφίνονται ως άσκηση.

□

Έστω $\mathbb{F}$ ένα πεπερασμένο σώμα χαρακτηριστικής p με $\mid \mathbb{F} \mid = p^n = q$. Η πολλαπλασιαστική του ομάδα περιέχει $q-1$ το πλήθος στοιχεία, οπότε για κάθε στοιχείο $a \in \mathbb{F}$ ισχύει $a^{q-1} = 1$, [3] δηλαδή $a^q = a$ για κάθε $a \in \mathbb{F}$. Από τη σχέση αυτή βλέπουμε ότι κάθε στοιχείο του σώματος $\mathbb{F}$ είναι ρίζα του πολυωνύμου

[3] Εδώ χρησιμοποιούμε, χωρίς να αποδεικνύουμε, το εξής αποτέλεσμα από τη Θεωρία Ομάδων. " Έστω G πεπερασμένη ομάδα, τότε για κάθε $g \in G$ ισχύει $g^{|G|} = 1$. "

$x^q - x$, επειδή δε το πλήθος των ριζών του $x^q - x$ είναι το πολύ q έχουμε ότι το σώμα $\mathbb{F}$ είναι τόσο το σύνολο ριζών του $x^q - x$, όσο και το σώμα ριζών του. Δηλαδή έχουμε αποδείξει ότι κάθε σώμα $\mathbb{F}$ με q το πλήθος στοιχεία είναι σώμα ριζών του πολυωνύμου $x^q - x$. Έχουμε όμως αναφέρει (Θεώρημα Α΄.2.30), ότι δύο σώματα ριζών ενός πολυωνύμου είναι ισόμορφα, επομένως έπεται ότι όλα τα πεπερασμένα σώματα με το ίδιο πλήθος στοιχείων είναι ισόμορφα.

Προηγουμένως αποδείξαμε ότι ένα πεπερασμένο σώμα είναι το σώμα ριζών ενός πολυωνύμου. Θα δείξουμε ότι για κάθε πρώτο p και κάθε θετικό ακέραιο n υπάρχει ένα σώμα $\mathbb{F}$ με $p^n = q$ το πλήθος στοιχεία.

Έστω $x^q - x \in \mathbb{Z}_p[x]$ και $\mathbb{E}$ το σώμα ριζών του. Για δύο ρίζες $\zeta, \xi \in \mathbb{E}$ δεν είναι δύσκολο να δούμε ότι $(\zeta \pm \xi)^q = \zeta \pm \xi$ (δες το Λήμμα Α΄.3.1). Επίσης $(\zeta \cdot \xi^{-1})^q = \zeta \cdot \xi^{-1}$. Δηλαδή τα $\zeta \pm \xi$ και $\zeta \cdot \xi^{-1}$ είναι ρίζες του πολυωνύμου $x^q - x$. Άρα, αν K είναι το σύνολο ριζών του $x^q - x$, τότε το K είναι σώμα που περιέχεται στο $\mathbb{E}$, δηλαδή $\mathrm{K} = \mathbb{E}$.

Το $x^q - x$ όμως έχει διακεκριμένες ρίζες. Πράγματι, η παράγωγος του $x^q - x$ είναι ίση με $(x^q - x)' = qx^{q-1} - 1 = -1 \in \mathbb{Z}_p[x]$, οπότε από το Πόρισμα Α΄.2.33 έχουμε ότι οι ρίζες του $x^q - x$ είναι διακεκριμένες. Επομένως το σώμα ριζών $\mathbb{E}$ έχει $q = p^n$ το πλήθος στοιχεία.

Τα προηγούμενα αποτελούν την απόδειξη του επομένου θεωρήματος.

Θεώρημα Α΄.3.2. *Για κάθε δύναμη ενός πρώτου αριθμού ($q = p^n$) υπάρχει μοναδικό (μέσω ισομορφισμού) σώμα $\mathbb{F}$ με $q = p^n$ το πλήθος στοιχεία, το οποίο είναι το σώμα (και σύνολο) ριζών του πολυωνύμου $x^q - x \in \mathbb{Z}_p[x]$.*

Α΄.3.2 Τα υποσώματα ενός πεπερασμένου σώματος

Έστω $\mathbb{F}$ ένα πεπερασμένο σώμα με $q = p^n$ το πλήθος στοιχεία και $\mathbb{K}$ ένα υπόσωμά του. Το $\mathbb{K}$ έχει p^d το πλήθος στοιχεία. Θα δείξουμε ότι το d διαιρεί το n.

Πράγματι, από τη σχέση (σελίδα 165) που μας δίνει το βαθμό διαδοχικών επεκτάσεων, έχουμε ότι $d \mid n$.

Αντίστροφα, έστω d ένας διαιρέτης του n, θα δείξουμε ότι υπάρχει ένα (μοναδικό) υπόσωμα $\mathbb{K}$ του $\mathbb{F}$ με p^d το πλήθος στοιχεία.

Από τη σχέση $d \mid n$ έπεται ότι $p^d - 1 \mid p^n - 1$ (γιατί;) Οπότε έχουμε $x^{p^d-1} - 1 \mid x^{p^n-1} - 1$, δηλαδή $x^{p^d} - x \mid x^{p^n} - x$. Το σώμα $\mathbb{F}$ είναι το σώμα ριζών του πολυωνύμου $x^{p^n} - x$, επομένως περιέχει το σώμα ριζών, έστω $\mathbb{K}$, του πολυωνύμου $x^{p^d} - x$. Το σώμα δεν μπορεί να περιέχει και άλλο σώμα με p^d το πλήθος στοιχεία, διότι τότε θα είχαμε περισσότερες ρίζες για το πολυώνυμο $x^{p^d} - x$ απ' ότι είναι ο βαθμός του.

Θεώρημα Α΄.3.3. *Έστω $\mathbb{F}$ ένα πεπερασμένο σώμα με $q = p^n$ το πλήθος στοιχεία. Το πλήθος των υποσωμάτων του $\mathbb{F}$ είναι ίσο με το πλήθος των θετικών διαιρετών του n.*

Απόδειξη. Η απόδειξη έχει προηγηθεί.

□

Θεώρημα Α΄.3.4. *Η πολλαπλασιαστική ομάδα ενός πεπερασμένου σώματος είναι κυκλική.*

Απόδειξη. Έστω $\mathbb{F}$ ένα πεπερασμένο σώμα με $q = p^n$ το πλήθος στοιχεία. Η πολλαπλασιαστική του ομάδα είναι αβελιανή και έχει $q-1$ το πλήθος στοιχεία. Υποθέτουμε ότι δεν είναι κυκλική, δηλαδή κανένα στοιχείο της δεν έχει τάξη ίση με $q-1$. Τότε (σύμφωνα με το επόμενο Λήμμα) υπάρχει $1 < r < q-1$ έτσι ώστε για κάθε μη μηδενικό στοιχείο a του σώματος $\mathbb{F}$ να ισχύει $a^r = 1$, δηλαδή κάθε μη μηδενικό στοιχείο του $\mathbb{F}$ είναι ρίζα του πολυωνύμου $x^r - 1$, αυτό είναι άτοπο, διότι ένα πολυώνυμο δεν μπορεί να έχει περισσότερες ρίζες από το βαθμό του. Άρα αναγκαστικά $r = q-1$ και η πολλαπλασιαστική ομάδα του $\mathbb{F}$ είναι κυκλική.
□

Το Λήμμα που επικαλούμαστε στην προηγούμενη απόδειξη χρησιμοποιεί ορισμένα αποτελέσματα από τη στοιχειώδη θεωρία των αβελιανών ομάδων.

Λήμμα Α΄.3.5. *Έστω G πεπερασμένη αβελιανή ομάδα και ένα $a \in G$ με την μεγαλύτερη δυνατή τάξη, έστω r, τότε $g^r = 1$ για κάθε $g \in G$.*

Απόδειξη. Υποθέτουμε ότι υπάρχει ένα $b \in G$ με τάξη ίση με s, η οποία δεν διαιρεί την τάξη του a.
Υποθέτουμε ότι το r και το s είναι πρώτα μεταξύ τους, τότε προφανώς η τάξη του στοιχείου $a \cdot b$ είναι ίση με το γινόμενο rs (γιατί;). Αυτό είναι άτοπο διότι υποθέσαμε ότι το r είναι η μεγαλύτερη δυνατή τάξη των στοιχείων της G.
Έστω ότι υπάρχει ένας πρώτος διαιρέτης p του s, ο οποίος δεν διαιρεί το r, τότε τα στοιχεία a και $b^{s/p}$ έχουν τάξεις r και p αντίστοιχα, επομένως το στοιχείο $a \cdot b^{s/p}$ έχει τάξη ίση με rp, πάλι άτοπο.
Απομένει η περίπτωση, όπου κάθε πρώτος διαιρέτης του s είναι και διαιρέτης του r. Επειδή έχουμε υποθέσει ότι η τάξη του b δεν διαιρεί την τάξη του a, υπάρχει πρώτος p τέτοιος ώστε η μεγαλύτερη δυνατή δύναμή του, έστω p^ν, που διαιρεί το s να είναι (γνήσια) μεγαλύτερη από τη μεγαλύτερη δυνατή δύναμή του , έστω p^λ που διαιρεί το r, δηλαδή $\nu > \lambda$. Η τάξη του στοιχείου a^λ είναι ίση με r/p^λ και η τάξη του στοιχείου b^{s/p^ν} είναι ίση με p^ν. Τα r/p^λ και p^ν όμως είναι πρώτα μεταξύ τους, επομένως η τάξη του στοιχείου $a^\lambda \cdot b^{s/p^\nu}$ είναι ίση με το γινόμενο $(r/p^\lambda)p^\nu$ το οποίο είναι μεγαλύτερο από το r, άτοπο.

Άρα τελικά δεν υπάρχει στοιχείο της ομάδας G με τάξη που να μην διαιρεί την τάξη του στοιχείου a.

□

Το προηγούμενο θεώρημα μας επιτρέπει να περιγράφουμε τα στοιχεία ενός πεπερασμένου σώματος ως δυνάμεις ενός μόνο στοιχείου του, του γεννήτορα της πολλαπλασιαστικής ομάδας.

Ένας γεννήτορας της πολλαπλασιαστικής ομάδας $\mathbb{F}^* = \mathbb{F} \setminus \{0\}$ θα ονομάζεται **πρωταρχικό** στοιχείο του σώματος.

Έστω $\mathbb{F}$ ένα πεπερασμένο σώμα με $q = p^n$ το πλήθος στοιχεία και c ένα πρωταρχικό στοιχείο. Το c δεν είναι το μοναδικό πρωταρχικό στοιχείο του $\mathbb{F}$. Μια δύναμη του c για να είναι πρωταρχικό στοιχείο πρέπει να είναι γεννήτορας της κυκλικής ομάδας $\mathbb{F}^*$, δηλαδή πρέπει να έχει τάξη ίση με $q-1$. Ως γνωστόν όμως η τάξη του c^r είναι ίση με την τάξη του c αν και μόνο αν το r και το $q-1$ είναι πρώτα μεταξύ τους, επομένως υπάρχουν τόσα πρωταρχικά στοιχεία όσο το πλήθος $\varphi(q-1)$ [4] των ακεραίων $1 \leq r \leq q-1$ οι οποίοι είναι πρώτοι προς το $q-1$.

Από την άλλη πλευρά γνωρίζουμε ότι κάθε πεπερασμένο σώμα είναι το σώμα ριζών ενός πολυωνύμου. Θα δούμε πώς μπορούμε να συνδυάσουμε τα πρωταρχικά στοιχεία ένος σώματος με τις ρίζες πολυωνύμων.

Έστω c ένα πρωταρχικό στοιχείο του $\mathbb{F}$, τότε προφανώς ισχύει $\mathbb{F} = \mathbb{Z}_p(c)$. Ο βαθμός της επέκτασης $[\mathbb{F} : \mathbb{Z}_p]$ είναι ίσος με το βαθμό του ελαχίστου πολυωνύμου $m_c(x) \in \mathbb{Z}_p[x]$ του c (βλέπε Σχόλιο Α΄.2.25). Επίσης από την Πρόταση Α΄.2.21 έχουμε ότι $\mathbb{F} = \mathbb{Z}_p(c) \simeq \mathbb{Z}_p[x]/\langle\, m_c(x)\,\rangle$. Επομένως κάθε στοιχείο του $\mathbb{F}$ θα μπορούσε να εκφρασθεί ως η τιμή ενός πολυωνύμου στη θέση c (βλέπε Πρόταση Α΄.2.22).

Στο επόμενο παράδειγμα θα περιγράψουμε τα στοιχεία ενός σώματος $\mathbb{F}$ με 16 στοιχεία.

Παράδειγμα Α΄.3.6. Έστω το σώμα $\mathbb{F}$ με 16 στοιχεία.

Το σώμα $\mathbb{F}$ είναι το σώμα ριζών του πολυωνύμου $x^{2^4} - x \in \mathbb{Z}_2[x]$ (Θεώρημα Α΄.3.2).

Έστω το πολυώνυμο $x^4 + x^3 + x^2 + x + 1 \in \mathbb{Z}_2[x]$. Το πολυώνυμο αυτό είναι ανάγωγο επί του $\mathbb{Z}_2[x]$ (μπορείτε να κάνετε τον έλεγχο). Επομένως ο δακτύλιος πηλίκων $\mathbb{Z}_2[x]/\langle\, x^4 + x^3 + x^2 + x + 1\,\rangle$ είναι (ισόμορφος με) το σώμα $\mathbb{F}$. Έστω c μια ρίζα του $x^4 + x^3 + x^2 + x + 1$, τότε τα στοιχεία του $\mathbb{F}$ είναι τα

[4] Η συνάρτηση φ είναι η γνωστή συνάρτηση Euler, της οποίας η τιμή $\varphi(n)$ για κάθε θετικό ακέραιο αριθμό n παριστά το πλήθος των ακεραίων μεταξύ του 1 και του n οι οποίοι είναι πρώτοι προς τον n.

Για ιδιότητες της συνάρτησης του Euler παραπέμπουμε σε κάθε εγχειρίδιο της Θεωρίας Αριθμών

0, 1, c, $c+1$, c^2, c^2+1, c^2+c, c^2+c+1, c^3, c^3+1, c^3+c, c^3+c^2, c^3+c+1, c^3+c^2+1, c^3+c^2+c, c^3+c^2+c+1 .

Η ρίζα c του πολυωνύμου $x^4+x^3+x^2+x+1$ πληροί τη σχέση $c^4 = c^3+c^2+c+1$. Από στη σχέση αυτή βλέπουμε ότι $c^5 = c(c^3+c^2+c+1) = c^4+c^3+c^2+c = (c^3+c^2+c+1)+(c^3+c^2+c) = 1$, δηλαδή είναι τάξης 5. Άρα δεν είναι πρωταρχικό στοιχείο του σώματος $\mathbb{F}$.

Αν αντί του πολυωνύμου $x^4+x^3+x^2+x+1$ πάρουμε το πολυώνυμο $x^4+x+1 \in \mathbb{Z}_2[x]$, τότε το πολυώνυμο αυτό είναι ανάγωγο και επομένως πάλι έχουμε $\mathbb{Z}_2[x]/\langle x^4+x+1\rangle = \mathbb{F}$. Όπως προηγουμένως αν ζ είναι μια ρίζα του x^4+x+1, τότε μπορούμε να εκφράσουμε τα στοιχεία του $\mathbb{F}$ ως τις τιμές πολυωνύμων βαθμού το πολύ 3 στη θέση ζ. Εδώ όμως ισχύει $\zeta^4 = \zeta+1$. Από τη σχέση αυτή βλέπουμε ότι $\zeta^3 \neq 1$, όπως επίσης $\zeta^5 \neq 1$. Άρα η τάξη του ζ είναι ίση με 15. Δηλαδή το ζ είναι πρωταρχικό στοιχείο του $\mathbb{F}$ και τα υπόλοιπα μη μηδενικά στοιχεία του είναι οι δυνάμεις του ζ.

Θα μπορούσαμε να εκφράσουμε τα μη μηδενικά στοιχεία του $\mathbb{F}$ τόσο ως δυνάμεις του ζ, όσο και ως πολυώνυμα ως προς ζ. Δηλαδή έχουμε ζ, ζ^2, ζ^3, $\zeta^4 = \zeta+1$, $\zeta^5 = \zeta^4\cdot\zeta = (\zeta+1)\zeta = \zeta^2+\zeta$, $\ldots$, $\zeta^{15} = 1$.

Ενδιαφέρον είναι να προσπαθήσετε να βρείτε πώς εκφράζεται το ίδιο στοιχείο του σώματος $\mathbb{F}$ ως η τιμή ενός πολυωνύμου στη θέση c και ως μια δύναμη του ζ.

Ορισμός Α΄.3.7. *Έστω $\mathbb{F}$ ένα πεπερασμένο σώμα, $\mathbb{E}$ μια επέκτασή του και ζ ένα πρωταρχικό στοιχείο του $\mathbb{E}$. Το ελάχιστο πολυώνυμο του ζ επί του $\mathbb{F}$ θα λέγεται* **πρωταρχικό** *πολυώνυμο του $\mathbb{E}$ επί του $\mathbb{F}$.*

Στο προηγούμενο παράδειγμα βλέπουμε ότι το πολυώνυμο x^4+x+1 είναι πρωταρχικό πολυώνυμο για το σώμα με 16 στοιχεία επί του σώματος $\mathbb{Z}_2$.

Η εύρεση των πρωταρχικών πολυωνύμων ενός σώματος δεν είναι εύκολη. Στα επόμενα απλώς θα δούμε ορισμένες ιδιότητές τους.

Α΄.3.3 Ανάγωγα πολυώνυμα με συντελεστές από πεπερασμένα σώματα

Πριν μελετήσουμε ιδιότητες αναγώγων πολυωνύμων με συντελεστές από ένα πεπερασμένο σώμα θα αποδείξουμε την ύπαρξη αναγώγων πολυωνύμων με οποιονδήποτε βαθμό.

Θεώρημα Α΄.3.8. *Για κάθε πεπερασμένο σώμα $\mathbb{F}$ και κάθε θετικό ακέραιο αριθμό n υπάρχει ανάγωγο πολυώνυμο με συντελεστές από το $\mathbb{F}$ και βαθμό ίσο με n.*

Απόδειξη. Έστω q το πλήθος των στοιχείων του σώματος $\mathbb{F}$, το q είναι δύναμη ενός πρώτου αριθμού, έστω p. Επομένως το q^n είναι δύναμη πρώτου αριθμού, άρα υπάρχει σώμα έστω $\mathbb{E}$ με q^n το πλήθος στοιχεία (Θεώρημα Α΄.3.2), το σώμα

$\mathbb{E}$ είναι επέκταση του σώματος $\mathbb{F}$. Έστω ζ ένα πρωταρχικό στοιχείο του $\mathbb{E}$, τότε $\mathbb{F}(\zeta) = \mathbb{E}$. Επομένως από τη σχέση $[\mathbb{E} : \mathbb{F}] = [\mathbb{F}(\zeta) : \mathbb{F}] = n$ έχουμε ότι ο βαθμός του ελαχίστου πολυωνύμου του ζ επί του $\mathbb{F}$ είναι ίσος με n.

□

Παρατήρηση Α΄.3.9. Από την προηγούμενη απόδειξη έπεται ότι για κάθε θετικό ακέραιο n δεν υπάρχει μόνο ανάγωγο πολυώνυμο με συντελεστές από ένα πεπερασμένο σώμα με βαθμό n, αλλά ένα πρωταρχικό πολυώνυμο βαθμού n.

Θα περιγράψουμε το σώμα ριζών ένος αναγώγου πολυωνύμου με συντελεστές από ένα πεπερασμένο σώμα.

Θεώρημα Α΄.3.10. *Έστω $\mathbb{F}$ ένα πεπερασμένο σώμα με q το πλήθος στοιχεία και $\sigma(x) \in \mathbb{F}[x]$ ένα ανάγωγο πολυώνυμο βαθμού d. Αν ξ είναι μια ρίζα του, τότε το σώμα ριζών του $\sigma(x)$ είναι το σώμα $\mathbb{F}(\xi)$.*

Απόδειξη. Έστω $\mathbb{E}$ το σώμα ριζών του $\sigma(x)$ και ξ μια ρίζα του. Προφανώς έχουμε ότι $\mathbb{F} \leq \mathbb{F}(\xi) \leq \mathbb{E}$. Ο βαθμός επέκτασης $[\mathbb{F}(\xi) : \mathbb{F}]$ είναι ίσος με d. Επομένως το σώμα $\mathbb{F}(\xi)$ έχει q^d το πλήθος στοιχεία και είναι το σώμα (σύνολο) ριζών του πολυωνύμου $x^{q^d} - x$ (Θεώρημα Α΄.3.2). Μια από τις ρίζες του $x^{q^d} - x$ είναι και το ξ, άρα το ανάγωγο πολυώνυμο $\sigma(x)$, που έχει και αυτό ρίζα το ξ, διαιρεί το $x^{q^d} - x$ (γιατί;). Επομένως όλες οι ρίζες του $\sigma(x)$ είναι και ρίζες του $x^{q^d} - x$, δηλαδή $\mathbb{F}(\xi) = \mathbb{E}$.

□

Πόρισμα Α΄.3.11. *Έστω $\mathbb{F}$ ένα πεπερασμένο σώμα με q το πλήθος στοιχεία και $\sigma(x) \in \mathbb{F}[x]$ ένα ανάγωγο πολυώνυμο βαθμού d. Το $\sigma(x)$ διαιρεί το πολυώνυμο $x^{q^n} - x$ αν και μόνο αν ο d διαιρεί τον n.*

Απόδειξη. Έστω $\mathbb{K}$ το σώμα ριζών του πολυωνύμου $\sigma(x)$ και $\mathbb{E}$ το σώμα ριζών του πολυωνύμου $x^{q^n} - x$. Από το προηγουμενο θεώρημα έπεται ότι το $\mathbb{K}$ έχει q^d το πλήθος στοιχεία. Από την απόδειξη του Θεωρήματος Α΄.3.3 έπεται ότι το $\mathbb{K}$ είναι υπόσωμα του $\mathbb{E}$ αν και μόνο αν το d διαιρεί το n.

Επομένως η απόδειξη ανάγεται στο ότι το ανάγωγο πολυώνυμο $\sigma(x)$ διαιρεί το $x^{q^n} - x$ αν και μόνο αν $\mathbb{K} \leq \mathbb{E}$.
Προφανώς αν το $\sigma(x)$ διαιρεί το $x^{q^n} - x$, τότε κάθε ρίζα του $\sigma(x)$ είναι και ρίζα του $x^{q^n} - x$, οπότε $\mathbb{K} \leq \mathbb{E}$.

Αντίστροφα, αν $\mathbb{K} \leq \mathbb{E}$, τότε επειδή το $\mathbb{E}$ είναι το σύνολο ριζών του $x^{q^n} - x$, κάθε ρίζα του $\sigma(x)$ είναι και ρίζα του $x^{q^n} - x$. Το $\sigma(x)$ όμως είναι ανάγωγο, άρα είναι το ελάχιστο πολυώνυμο (πολλαπλασιασμένο ίσως με ένα στοιχείο του σώματος $\mathbb{F}$) μιας ρίζας του $x^{q^n} - x$, επομένως διαιρεί το $x^{q^n} - x$. □

Στο Θεώρημα Α΄.3.10 είδαμε ότι αν $\mathbb{F}$ ένα πεπερασμένο σώμα με q το πλήθος στοιχεία και $\sigma(x) \in \mathbb{F}[x]$ ένα ανάγωγο πολυώνυμο βαθμού d, τότε το σώμα ριζών του $\sigma(x)$ προκύπτει με την επισύναψη μόνο μιας ρίζας ξ στο σώμα $\mathbb{F}$.

Μπορούμε να λεπτολογίσουμε περισσότερο και να υπολογίσουμε όλες τις ρίζες ενός αναγώγου πολυωνύμου, αρκεί να γνωρίζουμε μόνο μία από αυτές.

Θεώρημα Α΄.3.12. *Έστω $\mathbb{F}$ ένα πεπερασμένο σώμα με q το πλήθος στοιχεία και $\sigma(x) \in \mathbb{F}[x]$ ένα ανάγωγο πολυώνυμο βαθμού d. Αν ξ είναι μια ρίζα του, τότε οι υπόλοιπες ρίζες του $\sigma(x)$ είναι οι ξ^q, ξ^{q^2}, ... , $\xi^{q^{d-1}}$.*

Μάλιστα δε ο d είναι ο μικρότερος θετικός ακέραιος με την ιδιότητα $\xi^{q^d} = \xi$.

Απόδειξη. Το πεπερασμένο σώμα $\mathbb{F}$ έχει q το πλήθος στοιχεία και το q είναι ίσο με μια δύναμη ενός πρώτου p, την χαρακτηριστική του σώματος. Από το Λήμμα Α΄.3.1 και το γεγονός ότι $a^q = a$ για κάθε $a \in \mathbb{F}$ έπεται εύκολα ότι $\sigma(\xi^q) = (\sigma(\xi))^q = 0$. Δηλαδή το ξ^q είναι ρίζα του $\sigma(x)$. Όμοια αποδεικνύεται ότι τα ξ^{q^2}, ... , $\xi^{q^{d-1}}$ είναι ρίζες του $\sigma(x)$.

Για να τελειώσουμε πρέπει να αποδείξουμε ότι οι ρίζες ξ, ξ^q, ξ^{q^2}, ... , $\xi^{q^{d-1}}$ είναι διακεκριμένες. Υποθέτουμε ότι $\xi^{q^\kappa} = \xi^{q^\lambda}$ με $0 \leq \kappa < \lambda \leq d-1$, τότε $\xi^{q^\kappa} = \xi^{q^\lambda} = (\xi^{q^\kappa})^{q^{\lambda-\kappa}}$, δηλαδή $(\xi^{q^\kappa})^{q^{\lambda-\kappa}} - \xi^{q^\kappa} = 0$. Από την τελευταία σχέση έχουμε ότι το ξ^{q^κ} είναι ρίζα του πολυωνύμου $x^{q^{\lambda-\kappa}} - x$. Άρα το ξ^{q^κ} είναι κοινή ρίζα του ανάγωγου πολυωνύμου $\sigma(x)$ και του πολυωνύμου $x^{q^{\lambda-\kappa}} - x$. Δηλαδή το $\sigma(x)$ διαιρεί το $x^{q^{\lambda-\kappa}} - x$. Από το Πόρισμα Α΄.3.11 έπεται ότι το d πρέπει να διαιρεί το $\lambda - \kappa$, άτοπο.

□

Παρατήρηση Α΄.3.13. Το σώμα ριζών του αναγώγου πολυωνύμου $\sigma(x) \in \mathbb{F}[x]$ βαθμού d έχει q^d το πλήθος στοιχεία, επομένως η πολλαπλασιαστική του ομάδα έχει $q^d - 1$ το πλήθος στοιχεία. Οι δυνάμεις q^i είναι πρώτες ως προς τον $q^d - 1$, άρα όλες οι ρίζες ξ, ξ^q, ξ^{q^2}, ... , $\xi^{q^{d-1}}$ του πολυωνύμου $\sigma(x)$ έχουν την ίδια τάξη ως στοιχεία της πολλαπλασιαστικής ομάδας του σώματος ριζών του.

Το προηγούμενο θεώρημα θα μπορούσε να χρησιμεύσει στον υπολογισμό του ελαχίστου πολυωνύμου $m_c(x) \in \mathbb{F}[x]$ ενός αλγεβρικού στοιχείου c, το οποίο βρίσκεται σε μια επέκταση $\mathbb{E}$ του $\mathbb{F}$.

Πόρισμα Α΄.3.14. *Έστω $\mathbb{F}$ ένα πεπερασμένο σώμα με q το πλήθος στοιχεία και c ένα αλγεβρικό στοιχείο επί του $\mathbb{F}$. Το ελάχιστο πολυώνυμο του c είναι το πολυώνυμο $m_c(x) = (x-c)(x-c^q)\cdots(x-c^{q^{d-1}})$, όπου d είναι ο μικρότερος θετικός ακέραιος με την ιδιότητα $c^{q^d} = c$. Μάλιστα δε τα c, c^q, $\cdots$, $c^{q^{d-1}}$ έχουν το ίδιο ελάχιστο πολυώνυμο.*

Παρατήρηση Α΄.3.15. Στη σχέση $m_c(x) = (x-c)(x-c^q)\cdots(x-c^{q^{d-1}})$ ο πολλαπλασιασμός στο δεύτερο μέρος γίνεται σε μια επέκταση του σώματος $\mathbb{F}$ (συγκεκριμένα στο σώμα ριζών $\mathbb{F}(c)$ του $m_c(x)$), αλλά οι συντελεστές του $m_c(x)$, μετά τις πράξεις και την αναγωγή ομοίων όρων βρίσκονται στο σώμα $\mathbb{F}$.

Παράδειγμα Α΄.3.16. Στο παράδειγμα Α΄.3.6 περιγράφοντας τα στοιχεία ενός σώματος $\mathbb{F}$ με 16 στοιχεία είχαμε υπολογίσει δύο ελάχιστα πολυώνυμα στοιχείων του επί του $\mathbb{Z}_2$. Εδώ θα υπολογίσουμε τα ελάχιστα πολυώνυμα για όλα τα στοιχεία του.

Είχαμε δει ότι το πολυώνυμο x^4+x+1 είναι πρωταρχικό πολυώνυμο. Έστω ζ ένα πρωταρχικό στοιχείο του σώματος $\mathbb{F}$, το οποίο είναι ρίζα του x^4+x+1. Επιπλέον το ζ είναι ένας γεννήτορας της πολαπλασιαστικής ομάδας του σώματος. Παρατηρούμε ότι:
(i) $\zeta^{2^4} = \zeta$, άρα τα $\zeta, \zeta^2, \zeta^4, \zeta^8$ έχουν το ίδιο ελάχιστο πολυώνυμο $m_\zeta(x) = (x-\zeta)(x-\zeta^2)(x-\zeta^4)(x-\zeta^8)$.

(ii) $(\zeta^3)^{2^4} = \zeta^3$, άρα τα $\zeta^3, \zeta^6, \zeta^{12}, \zeta^{24} = \zeta^9$ έχουν το ίδιο ελάχιστο πολυώνυμο $m_{\zeta^3}(x) = (x-\zeta^3)(x-\zeta^6)(x-\zeta^{12})(x-\zeta^9)$.

(iii) $(\zeta^5)^{2^2} = \zeta^5$, άρα τα ζ^5, ζ^{10} έχουν το ίδιο ελάχιστο πολυώνυμο $m_{\zeta^5}(x) = (x-\zeta^5)(x-\zeta^{10})$.

(iv) $(\zeta^7)^{2^4} = \zeta^7$, άρα τα $\zeta^7, \zeta^{14}, \zeta^{28} = \zeta^{13}, \zeta^{56} = \zeta^{11}$ έχουν το ίδιο ελάχιστο πολυώνυμο $m_{\zeta^7}(x) = (x-\zeta^7)(x-\zeta^{14})(x-\zeta^{13})(x-\zeta^{11})$.

Χρησιμοποιώντας το γεγονός ότι το ζ είναι ρίζα του x^4+x+1, δηλαδή $\zeta^4 = \zeta+1$, μπορούμε να υπολογίσουμε τα ελάχιστα πολυώνυμα. Συγκεκριμένα έχουμε

$m_\zeta(x) = x^4+x+1$
$m_{\zeta^3}(x) = x^4+x^3+x^2+x+1$
$m_{\zeta^5}(x) = x^2+x+1$
$m_{\zeta^7}(x) = x^4+x^3+1$

Από τα πολυώνυμα αυτά μόνο τα $m_\zeta(x) = x^4+x+1$ και $m_{\zeta^7}(x) = x^4+x^3+1$ είναι πρωταρχικά.

Δεν είναι εύκολο να υπολογίσουμε όλα τα ανάγωγα πολυώνυμα ενός συγκεκριμένου βαθμού επί ενός πεπερασμένου σώματος. Θα μπορούσαμε όμως να υπολογίσουμε το πλήθος τους.

Θεώρημα Α΄.3.17. *Έστω $\mathbb{F}$ ένα πεπερασμένο σώμα με q το πλήθος στοιχεία και n ένας θετικός ακέραιος. Το πολυώνυμο $x^{q^n}-x$ είναι το γινόμενο όλων των αναγώγων πολυωνύμων επί του $\mathbb{F}$, των οποίων ο βαθμός είναι διαιρέτης του n.*

Απόδειξη. Γνωρίζουμε ότι (Πόρισμα Α΄.3.11) ένα ανάγωγο πολυώνυμο διαιρεί το $x^{q^n}-x$ αν και μόνο αν ο βαθμός του διαιρεί το n. Επομένως η ανάλυση

του $x^{q^n} - x$ σε γινόμενο αναγώγων πολυωνύμων περιλαμβάνει όλα τα ανάγωγα πολυώνυμα με βαθμό που είναι διαιρέτης του n.

Ένας ανάγωγος παράγοντας του $x^{q^n} - x$ εμφανίζεται μία μόνο φορά στην ανάλυση του $x^{q^n} - x$, διότι το $x^{q^n} - x$ δεν έχει πολλαπλές ρίζες (βλέπε την απόδειξη του Θεωρήματος Α΄.3.2). Άρα πράγματι ισχύει ο ισχυρισμός του θεωρήματος. □

Έστω $\alpha_q(d)$ ο αριθμός των αναγώγων πολυωνύμων βαθμού d επί του πεπερασμένου σώματος $\mathbb{F}$ με q το πλήθος στοιχεία. Από το προηγούμενο θεώρημα έπεται ότι $q^n = \sum_{d|n} d \cdot \alpha_q(d)$.

Στην τελευταία σχέση αν εφαρμόσουμε τον τύπο αντιστροφής του Möbius [5] έχουμε ότι

$$\alpha_q(n) = \frac{1}{n} \sum_{d|n} \mu(d) q^{n/d} .$$

Για παράδειγμα το πλήθος των αναγώγων πολυωνύμων βαθμού 12 είναι ίσο με $\alpha_q(12) = \frac{1}{12}(\mu(1)q^{12} + \mu(2)q^6 + \mu(3)q^4 + \mu(4)q^3 + \mu(6)q^2 + \mu(12)q) = \frac{1}{12}(q^{12} - q^6 - q^4 + q^2)$.

Πρόταση Α΄.3.18. *Έστω $\mathbb{F}$ ένα πεπερασμένο σώμα με q το πλήθος στοιχεία ένα μονικό ανάγωγο πολυωνυμο $f(x) \in \mathbb{F}[x]$ βαθμού d είναι πρωταρχικό (για κάποια επέκταση $\mathbb{E}$ του $\mathbb{F}$) αν και μόνο αν το $f(x)$ διαιρεί το πολυώνυμο $x^{q^d-1} - 1$ και το $f(x)$ δεν διαιρεί κανένα πολυώνυμο της μορφής $x^k - 1$ για κάθε $k < q^d - 1$.*

Απόδειξη. Έστω $f(x) \in \mathbb{F}[x]$ ένα ανάγωγο πολυώνυμο βαθμού d. Από το Πόρισμα Α΄.3.11 έχουμε ότι το $f(x)$ διαιρεί το $x^{q^d-1} - 1$. Μάλιστα δε ο d είναι ο μικρότερος θετικός ακέραιος s με την ιδιότητα το $f(x)$ να διαιρεί το $x^{q^s-1} - 1$.

Το σώμα ριζών του πολυωνύμου $f(x)$ είναι μια επέκταση $\mathbb{E}$ του $\mathbb{F}$ με q^d το πλήθος στοιχεία, Υποθέτουμε ότι το $f(x)$ δεν διαιρεί κανένα πολυώνυμο της μορφής $x^k - 1$ για κάθε $k < q^d - 1$. Άρα καμία ρίζα ξ του $f(x)$ δεν έχει την ιδιότητα $\xi^k = 1$ για $k < q^d - 1$. Αλλά κάθε ρίζα ζ του $f(x)$ έχει την ιδιότητα $\zeta^{q^d-1} = 1$. Δηλαδή το ζ είναι γεννήτορας της πολλαπλασιαστικής ομάδας του

[5] Η συνάρτηση του Möbius για έναν θετικό ακέραιο m ορίζεται ως εξής

$$\mu(m) = \begin{cases} 1 & \text{αν } m = 1 \\ (-1)^k & \text{αν } m = p_1 p_2 \cdots p_k \text{ όπου οι } p_i \text{ είναι διακεκριμένοι πρώτοι} \\ 0 & \text{διαφορετικά} \end{cases} .$$

Ο τύπος αντιστροφής του Möbius είναι ο εξής

Αν $g(n) = \sum_{d|n} f(d)$, τότε έπεται ότι $f(n) = \sum_{d|n} g(n/d)\mu(d)$.

Για ιδιότητες της συνάρτησης του Möbius παραπέμπουμε σε κάθε εγχειρίδιο της Θεωρίας Αριθμών.

σώματος $\mathbb{E}$. Συνεπώς το $f(x)$ είναι πρωταρχικό πολυώνυμο του σώματος ριζών του $\mathbb{E}$.

Υποθέτουμε τώρα ότι το ανάγωγο πολυώνυμο $f(x)$ είναι πρωταρχικό πολυώνυμο σε μια επέκταση $\mathbb{E}$ του $\mathbb{F}$, δηλαδή το ελάχιστο πολυώνυμο ενός πρωταρχικού στοιχείου ζ του $\mathbb{E}$. Θα δείξουμε ότι το $f(x)$ δεν διαιρεί κανένα πολυώνυμο της μορφής $x^k - 1$ για κάθε $k < q^d - 1$.

Εφ' όσον το ζ είναι ρίζα του $f(x)$ οι άλλες ρίζες του είναι οι ζ^q, ζ^{q^2}, ... , $\zeta^{q^{d-1}}$. Επομένως το σώμα ριζών που περιέχει q^d το πλήθος στοιχεία περιέχεται στο σώμα $\mathbb{E}$, το οποίο έχει το ίδιο πλήθος στοιχείων, άρα το $\mathbb{E}$ είναι το σώμα ριζών του $f(x)$. Το $f(x)$ δεν διαιρεί κανένα πολυνώνυμο της μορφής $x^k - 1$ για κάθε $k < q^d - 1$, διότι διαφορετικά θα είχαμε $\zeta^k = 1$, άτοπο, αφού η τάξη του ζ είναι ίση με $q^d - 1$.

□

Παρατήρηση Α΄.3.19. Στην προηγούμενη πρόταση αποδείξαμε ότι οι έννοιες πρωταρχικό πολυώνυμο και πρωταρχικό στοιχείο του σώματος ριζών του συνδέονται με το γεγονός ότι οι ρίζες του πρωταρχικού πολυωνύμου είναι πωταρχικά στοιχεία του σώματος ριζών του.

Α΄.3.4 Οι ρίζες της μονάδας επί πεπερασμένων σωμάτων

Έστω $\mathbb{F}$ ένα πεπερασμένο σώμα με q το πλήθος στοιχεία χαρακτηριστικής p (το q είναι μια δύναμη του p) και $x^n - 1 \in \mathbb{F}[x]$. Υποθέτουμε ότι $n = m \cdot p^k$ με το m να είναι πρώτο προς το p. Τότε προφανώς $x^n - 1 = x^{m \cdot p^k} - 1 = (x^m - 1)^{p^k}$, οπότε η αναζήτηση των ριζών (και γενικά η μελέτη) του $x^n - 1$ ανάγεται στην μελέτη του πολυωνύμου $x^m - 1$, όπου το m είναι πρώτο προς το p (και φυσικά προς το q). Στα επόμενα χωρίς άλλη μνεία θα υποθέτουμε ότι το n και το q είναι σχετικά πρώτοι.

Έστω $\mathbb{E}$ το σώμα ριζών του $x^n - 1 \in \mathbb{F}[x]$ και $\mathcal{E}_n$ το σύνολο ριζών του. Τα στοιχεία του $\mathcal{E}_n$ ονομάζονται **n−οστές ρίζες της μονάδας** επί του σώματος $\mathbb{F}$. Οι ρίζες του $x^n - 1$ είναι διακεκριμένες (γιατί;), επομένως το $\mathcal{E}_n$ είναι ένα υποσύνολο της πολλαπλασιαστικής ομάδας του σώματος ριζών $\mathbb{E}$ με n το πλήθος στοιχεία.

Πρόταση Α΄.3.20. *1. Το σύνολο $\mathcal{E}_n$ είναι μια κυκλική ομάδα τάξης n.*

2. Ο βαθμός επέκτασης $[\mathbb{E} : \mathbb{F}] = s$ είναι ο μικρότερος θετικός ακέραιος με την ιδιότητα $q^s \equiv 1 \bmod n$.

Απόδειξη. Έστω $\zeta, \xi \in \mathcal{E}_n$, τότε $(\zeta \cdot \xi^{-1})^n = \zeta^n \cdot (\xi^n)^{-1} = 1$. Άρα $\zeta \cdot \xi^{-1} \in \mathcal{E}_n$. Επομένως οι ρίζες του $x^n - 1$ αποτελούν μια (υπο)ομάδα της πολλαπλασιαστικής ομάδας του $\mathbb{E}$, η οποία όμως είναι κυκλική. Άρα και η $\mathcal{E}_n$ είναι κυκλική.

Το σώμα ριζών $\mathbb{E}$ έχει q^s το πλήθος στοιχεία, όπου s είναι ο βαθμός επέκτασης $[\mathbb{E} : \mathbb{F}]$. Οπότε η πολλαπλασιαστική ομάδα του $\mathbb{E}$ έχει $q^s - 1$ το πλήθος στοιχεία και επομένως η τάξη n της υποομάδας $\mathcal{E}_n$ διαιρεί το $q^s - 1$.

Έστω r θετικός ακέραιος έτσι ώστε το n να διαιρεί το $q^r - 1$, τότε το πολυώνυμο $x^n - 1$ διαιρεί το πολυώνυμο $x^{q^r-1} - 1$. Δηλαδή το σώμα ριζών $\mathbb{E}$ του πολυωνύμου $x^n - 1$ περιέχεται σε κάθε σώμα με q^r το πλήθος στοιχεία, αρκεί το n να διαιρεί το $q^r - 1$. Άρα είναι το σώμα με q^s το πλήθος στοιχεία, όπου s είναι ο μικρότερος θετικός ακέραιος έτσι ώστε το n να διαιρεί το $q^s - 1$.

□

Έστω ω ένας γεννήτορας της ομάδας $\mathcal{E}_n$ των $n-$οστών ριζών της ομάδας, τότε κάθε άλλη $n-$οστή ρίζα της μονάδας είναι της μορφής ω^i, $i = 0, 1, \ldots, n-1$. Μια τέτοια ρίζα θα λέγεται **πρωταρχική** $n-$οστή ρίζα της μονάδας . Μια άλλη πρωταρχική $n-$οστή ρίζα της μονάδας θα είναι της μορφής ω^k, όπου $\mu.\kappa.\delta.(n, k) = 1$ (γιατί;). Επομένως υπάρχουν $\varphi(n)$ το πλήθος πρωταρχικές ρίζες της μονάδας, όπου φ παριστά τη συνάρτηση του Euler.

Δεν πρέπει να συγχέουμε τις $n-$οστές πρωταρχικές ρίζες της μονάδας με τα πρωταρχικά στοιχεία του σώματος $\mathbb{E}$ ριζών του πολυωνύμου $x^n - 1$.

Έστω ω μια πρωταρχική $n-$οστή ρίζα της μονάδας και ζ ένα πρωταρχικό στοιχείο του $\mathbb{E}$. Τότε η τάξη του ζ είναι ίση με $q^s - 1$ και το ω είναι μια δύναμη του ζ, δηλαδή $\omega = \zeta^k$.

Γνωρίζουμε ότι η τάξη του ω είναι ίση με n. Από την άλλη πλευρά όμως η τάξη του ζ^k είναι ίση με $\frac{q^s-1}{\mu.\kappa.\delta.(k,q^s-1)}$. Αλλά το n διαιρεί το $q^s - 1$, δηλαδή $q^s - 1 = nr$. Οπότε η τελευταία σχέση γίνεται $\frac{q^s-1}{\mu.\kappa.\delta.(k,q^s-1)} = \frac{nr}{\mu.\kappa.\delta.(k,nr)}$. Επομένως το στοιχείο ζ^k είναι πωταρχική $n-$οστή ρίζα της μονάδας αν και μόνο αν $\frac{nr}{\mu.\kappa.\delta.(k,nr)} = n$, αν και μόνο αν $\mu.\kappa.\delta.(k, nr) = r$, αν και μόνο αν $k = rm$, οπου το m είναι πρώτο προς το n. Άρα αποδείξαμε το εξής θεώρημα.

Θεώρημα Α΄.3.21. *Έστω ζ ένα πρωταρχικό στοιχείο του $\mathbb{E}$, του σώματος ριζών του πολυωνύμου $x^n - 1 \in \mathbb{F}[x]$. Το σύνολο των πρωταρχικών $n-$οστών ριζών της μονάδος είναι το σύνολο*

$$\Omega = \{\, \zeta^k \mid k = \frac{q^s - 1}{n} m,\ m < n \text{ και } o \text{ είναι πρώτος προς τον } n \,\} .$$

Πόρισμα Α΄.3.22. *Έστω $\mathbb{F}$ ένα πεπερασμένο σώμα με q το πλήθος στοιχεία και $\mathbb{E}$ το σώμα ριζών του $x^n - 1 \in \mathbb{F}[x]$ με q^s το πλήθος στοιχεία. Αν Φ είναι το σύνολο των πρωταρχικών στοιχείων του σώματος $\mathbb{E}$, τότε $\Omega \cap \Phi = \emptyset$, εκτός εάν $n = q^s - 1$, οπότε $\Omega = \Phi$.*

Το προηγούμενο πόρισμα κάνει σαφή τη διάκριση μεταξύ πρωταρχικών ριζών του πολυωνύμου $x^n - 1$ και πρωταρχικών στοιχείων του σώματος ριζών του.

Έστω $\mathbb{F}$ ένα σώμα με q το πλήθος στοιχεία και $x^n - 1 \in \mathbb{F}[x]$. Επειδή οι ρίζες του $x^n - 1$ είναι διακεκριμένες, το πολυώνυμο $x^n - 1$ είναι το γινόμενο των διακεκριμένων ελαχίστων πολυωνύμων των αντίστοιχων ριζών του.

Έστω $\mathbb{E}$ το σώμα ριζών του $x^n - 1$. Το $\mathbb{E}$ έχει q^s το πλήθος στοιχεία. Αν ζ είναι ένα πρωταρχικό στοιχείο του $\mathbb{E}$, τότε από το προηγούμενο θεώρημα το στοιχείο $\omega = \zeta^{(q^s-1)/n}$ είναι μια πρωταρχική $n-$οστή ρίζα της μονάδας. Επομένως οι ρίζες του $x^n - 1$ είναι οι $1, \omega, \omega^2, \ldots, \omega^{n-1}$.

Το ελάχιστο πολυώνυμο $m_\omega(x)$ της ρίζας ω έχει ως ρίζες τις $\omega, \omega^q, \ldots, \omega^{q^{d-1}}$, όπου d είναι ο μικρότερος θετικός ακέραιος με την ιδιότητα $\omega^{q^d} = \omega$, δηλαδή $q^d \equiv 1 \bmod n$. Επομένως $m_\omega(x) = (x-\omega)(x-\omega^q)\cdots(x-\omega^{q^{d-1}})$. Όμοια για κάθε ρίζα ω^i το αντίστοιχο ελάχιστο πολυώνυμο είναι της μορφής $m_{\omega_i}(x) = (x-\omega^i)(x-\omega^{iq})\cdots(x-\omega^{iq^{d_i-1}})$, όπου d είναι ο μικρότερος θετικός ακέραιος με την ιδιότητα $\omega^{iq^{d_i}} = \omega^i$, δηλαδή $iq^{d_i} \equiv i \bmod n$

Ο προηγούμενος τρόπος παραγοντοποίησης του πολυωνύμου $x^n - 1$ έχει το μειονέκτημα ότι οι πράξεις πρέπει να γίνονται στο σώμα ριζών του.

Θα δούμε έναν άλλο τρόπο παραγοντοποίησης του πολυωνύμου $x^n - 1 \in \mathbb{F}[x]$.

Έστω ω μια πρωταρχική ρίζα του $x^n - 1$, όλες οι ρίζες είναι οι ω^k. Αν το k είναι πρώτο προς το n, τότε έχουμε μια άλλη πρωταρχική ρίζα. Αν το k δεν είναι πρώτο προς το n, τότε η τάξη $m = \frac{n}{\mu.\kappa.\delta.(k,\, n)}$ της ω^k ως στοιχείο της ομάδας $\mathcal{E}_n$ είναι ένας διαιρέτης του n. Δηλαδή η ω^k είναι $m-$οστή πρωταρχική ρίζα της μονάδος.

Αντίστροφα, για κάθε διαιρέτη m του n κάθε ρίζα του $x^m - 1$ είναι ρίζα του $x^n - 1$. Άρα τελικά όλες οι ρίζες του $x^n - 1$ είναι πρωταρχικές ρίζες στα πολυώνυμα $x^m - 1$ με m διαιρέτη του n.

Από τα προηγούμενα οδηγούμαστε στον επόμενο ορισμό.

Ορισμός Α΄.3.23. *Έστω $\mathbb{F}$ ένα σώμα με q το πλήθος στοιχεία και k ένας θετικός ακέραιος πρώτος προς τον q. Το* **κυκλοτομικό** *πολυώνυμο τάξης k επί του $\mathbb{F}$ είναι το μονικό πολυώνυμο $Q_k(x)$, του οποίου οι ρίζες είναι οι πρωταρχικές $k-$στές ρίζες της μονάδος.*

Γνωρίζουμε ότι οι πρωταρχικές $k-$στές ρίζες της μονάδας είναι $\varphi(k)$ το πλήθος, όπου φ είναι η συνάρτηση του Euler. Δηλαδή αν $\zeta_1, \zeta_2, \ldots, \zeta_{\varphi(k)}$ είναι οι πρωταρχικές $k-$στές ρίζες της μονάδας, τότε
$Q_k(x) = (x-\zeta_1)(x-\zeta_2)\cdots(x-\zeta_{\varphi(k)})$.

Από τη συζήτηση που προηγήθηκε του ορισμού έπεται άμεσα ότι
$x^n - 1 = \Pi_{d|n} Q_d(x)$.

Παρατηρήσεις Α΄.3.24. 1. Από τον τρόπο ορισμού των κυκλοτομικών πολυωνύμων δεν έπεται ότι οι συντελεστές τους είναι στοιχεία του σώματος $\mathbb{F}$. Αλλά αν $x^n-1 = m_1(x)\cdot m_2(x)\cdots m_\nu$ είναι η ανάλυση του x^n-1 σε γινόμενο αναγώγων πολυωνύμων επί του $\mathbb{F}$, τότε από τη σχέση $x^n-1 = m_1(x)\cdot m_2(x)\cdots m_\nu = \Pi_{d|n}Q_d(x)$, αν ζ είναι μια ρίζα ενός $Q_d(x)$, αυτή θα είναι ρίζα ενός (μόνο) $m_i(x)$. Οπότε οι ρίζες του $m_i(x)$ είναι οι ζ, ζ^q, $\ldots$, $\zeta^{q^{d-1}}$. Η ζ ως ρίζα του $Q_d(x)$ έχει τάξη ίση με d (ως πρωταρχική $d-$οστη ρίζα της μονάδας), οπότε όλες οι ρίζες ζ, ζ^q, $\ldots$, $\zeta^{q^{d-1}}$ του $m_i(x)$ έχουν τάξη ίση με d (γιατί;). Επομένως όλες είναι πρωταρχικές $d-$οστες ρίζες της μονάδας, άρα όλες είναι ρίζες του $Q_d(x)$, δηλαδή το $m_i(x)$ διαιρεί το $Q_d(x)$. Τελικά κάθε $Q_d(x)$ είναι το γινόμενο (κάποιων από τα) $m_i(x)\in\mathbb{F}[x]$, άρα και τα $Q_d(x)\in\mathbb{F}[x]$.

2. Υπάρχει ένας άλλος (αναδρομικός) τρόπος, με τον οποίο όχι μόνο διαπιστώνουμε ότι τα κυκλοτομικά πολυώνυμα έχουν συντελεστές από το σώμα $\mathbb{F}$, αλλά μπορούμε να τα υπολογίσουμε.

   $x^2-1 = Q_1(x)\,Q_2(x)$

   $x^3-1 = Q_1(x)\,Q_3(x)$

   $x^4-1 = Q_1(x)\,Q_2(x)\,Q_4(x)$

   $x^5-1 = Q_1(x)\,Q_5(x)$

   $x^6-1 = Q_1(x)\,Q_2(x)\,Q_3(x)\,Q_6(x)$

   και έπεται η συνέχεια.

   Οπότε έχουμε $Q_1(x) = x-1$, $Q_2(x) = x+1$, $Q_3(x) = x^2+x+1$, $Q_4(x) = \frac{x^4-1}{Q_1(x)\,Q_2(x)} = x^2+1$, $Q_5(x) = \frac{x^5-1}{Q_1(x)} = x^4+x^3+x^2+x+1$, $Q_6(x) = \frac{x^6-1}{Q_1(x)\,Q_2(x)\,Q_3(x)} = x^2-x+1$

   και έπεται η συνέχεια.

3. Επίσης με επαγωγή μπορούμε να αποδείξουμε ότι τα κυκλοτομοκά πολυώνυμα έχουν τους συντελεστές τους στο πρώτο σώμα $\mathbb{Z}_p$, όπου p είναι η χαρακτηριστική του σώματος $\mathbb{F}$ (προσπαθήστε το!).

4. Ο προηγούμενος τρόπος υπολογισμού των κυκλοτομικών πολυωνύμων είναι χρονοβόρος και λόγω της αναδρομικότητας μετά από ορισμένα βήματα στην πράξη είναι ατελέσφορος.

   Θα μπορούσαμε να υπολογίζουμε τα κυκλοτομικά πολυώνυμα απ' ευθείας για κάθε τάξη k. Εφαρμόζουμε τον τύπο αντιστροφής του Möbius (βλέπε σελίδα 191) στη σχέση $x^n-1 = \prod_{d|n}Q_d(x)$ και έχουμε ότι $Q_n(x) =$

$\prod_{d|n}(x^d-1)^{\mu(n/d)} = \prod_{d|n}(x^{n/d}-1)^{\mu(d)}$. Αλλά προσοχή! μερικοί από τους εκθέτες στο προηγούμενο γινόμενο ενδέχεται να είναι ίσοι με -1, οπότε πρέπει να γίνουν οι αντίστοιχες διαιρέσεις.

Παράδειγμα. Έστω $x^{15}-1 = Q_1(x)\,Q_3(x)\,Q_5(x)\,Q_{15}(x) \in \mathbb{Z}_2[x]$. Σύμφωνα με τα προηγούμενα έχουμε ότι $Q_{15}(x) = (x^{15}-1)\,(x^5-1)^{-1}\,(x^3-1)^{-1}\,(x-1) = \frac{(x^{15}-1)\,(x-1)}{(x^5-1)\,(x^3-1)} = x^8+x^7+x^5+x^4+x^3+x+1$.

Όμοια μπορείτε να υπολογίσετε και τα υπόλοιπα κυκλοτομικά πολυώνυμα.

Βιβλιογραφία

[1] Hall, J.I. *Notes on Coding Theory* (σε ηλεκτρονική μορφή) www.math.msu.edu\ ∼jhall

[2] Hamming, R. *"Coding and Information Theory"*, Prentice-Hall, Englewood Cliffs 1980.

[3] Hill, R. *"A First Course in Coding Theory"*, Oxford University Press, Oxford 1986.

[4] MacWilliams, F.J. - Sloane, N.J.A. *"The Theory of Error-correcting Codes"*, North-Holland, Amsterdam 1977.

[5] Pless, V. *"Introduction to the Theory of Error-Correcting Codes"*, Wiley, New York 1998.

[6] Pretzel, O. *"Error-Correcting Codes and Finite Fields"*, Oxford University Press, Oxford 1992.

[7] Roman, S. *"Coding and Information Theory"*, Springer-Verlag, 1992.

[8] van Lint, J.H. *"Introduction to Coding Theory"*, Springer-Verlag, 1999.

[9] Vermani, L. *"Elements of Algebraic Coding Theory"*, Chapman and Hall, London 1996.

Ευρετήριο

αύξηση κώδικα, 38
αδύναμος γεννήτορας, 122
αθόρυβος δίαυλος, 16
ακεραία περιοχή, 161
ακτίνα κάλυψης, 49
ακτίνα ομαδοποίησης, 48
αλφάβητο, 6
αμοιβαίο πολυώνυμο, 120
ανίχνευση λάθους, 25
αναστρέψιμος κώδικας, 126
αντιπροσωπευτική διάταξη, 85
αντιπροσωπος συμπλόκου, 84
αντιστρέψιμο στοιχείο, 159
απόσταση, 7
απαριθμητής βάρους, 96
αποκωδικοποίηση, 9
αρχή της μέγιστης πιθανότητας, 19
αρχή της πλησιέστερης λέξης, 23
αυτοδυϊκός κώδικας, 77
αυτοορθογώνιος κώδικας, 83

βάρος λέξης, 11
βέλτιστος κώδικας, 51
βαθμός επέκτασης, 167

γεννήτορας πίνακας, 61
γραμμικός κώδικας, 59

δίαυλος αμνήμων, 15
δίαυλος επικοινωνίας, 15
δακτύλιος κυρίων ιδεωδών, 165
δακτύλιος πηλίκων, 166
διόρθωση λάθους, 25
διαιρέτης του μηδενός, 161
διαχωρίσιμος κώδικας, 65
διασπορά βαρών, 96
δυϊκός κώδικας, 69
δυαδικός
    κώδικας, 8

ε.κ.π. πολυωνύμων, 178
ελάχιστη
    απόσταση, 24
ελάχιστο βάρος, 60
ελάχιστο πολυώνυμο, 181
επέκταση κώδικα, 36
επέκταση σώματος, 167
επαναληπτικός κώδικας, 40
επαυξημένος κώδικας, 38
εσωτερικό γινόμενο, 67
εξισώσεις ελέγχου ισοτιμίας, 69

ιδανικός παρατηρητής, 21
ιδεώδες, 163
ιδεώδες παραγόμενο, 164
ισοδύναμοι κώδικες, 35

κάθετα διανύσματα, 68
κύριο ιδεώδες, 165
κώδικας, 8
κώδικας p-αδικός, 8
κώδικας Hamming, 128
κώδικας Reed-Muller $r-$τάξης, 155

κώδικας Reed-Muller πρώτης τάξης, 151
κώδικας simplex, 132
κώδικας μηδενικού αθροίσματος, 37
κώδικες μέγιστης απόστασης, 99
κανόνας αποφασισιμότητας, 17
κλάσεις υπολοίπων, 158
κυκλοτομικό πολυώνυμο, 196
κωδικολέξη, 8
κωδικοποίηση, 9

λάθος, 14
λέξη, 6

μήκος
κώδικα, 10
μήκος λέξης, 7
μ.κ.δ.
πολυωνύμων, 172
μεγιστικός κώδικας, 42
μη πλήρης αποκωδικοποίηση, 23

ογκος σφαίρας, 46
ομομορφισμός δακτυλίων, 163
ορθογώνια διανύσματα, 68
ορθογώνιο συμπλήρωμα, 68

πίνακας Hamming, 128
πίνακας ανηγμένος κλιμακωτός, 64
πίνακας ελέγχου ισοτιμίας, 69
πίνακας μετάθεση, 36
πηγή, 8
πιθανότητες μετάδοσης, 15
πλήρης αποκωδικοποίηση, 23
πολλαπλότητα ρίζας, 184
πολυώνυμα
σχετικά πρώτα, 176
πολυώνυμο ελέγχου, 118
πολυώνυμο γεννήτορας, 107, 115
πολυωνυμικός κώδικας, 107
πρώτο σώμα, 168
πρωταρχική ρίζα της μονάδας, 195
πρωταρχικό πολυώνυμο, 189
πρωταρχικό στοιχείο, 188

ρίζα πολυωνύμου, 181

σύμπλοκο, 84, 166
σύμπτυξη κώδικα, 37
σύνδρομο, 91
σώμα, 162
σφαίρα, 45
σφαίρες κάλυψης, 49
σφαίρες ομαδοποίησης, 48
σμίκρυνση κώδικα, 38
στοιχειώδεις μετασχηματισμοί πίνακα, 66
συμμετρικός δίαυλος, 16
συμπύκνωση κώδικα, 39
συμπλήρωμα λέξης, 39
συνάρτηση αποκωδικοποίησης, 18
συνάρτηση κωδικοποίησης, 8
συνάρτηση μέγιστης πιθανότητας, 19
συστηματικός κώδικας, 65

τέλειος κώδικας, 49

ψηφίο ελέγχου ισοτιμίας, 37

χαρακτήρας, 6
χαρακτηριστική δακτυλίου, 161