Κώδικες Reed - Solomon

και

Βασικές Επεκτάσεις τους

Θεοδωρακόπουλος Στέφανος

Διπλωματική εργασία

Επιβλέπουσα Καθηγήτρια: Σοφία Λαμπροπούλου
Συνεπιβλέπων Καθηγητής: Αριστείδης Κοντογεώργης

Τριμελής Επιτροπή:

Σοφία Λαμπροπούλου	Καθηγήτρια ΕΜΠ	(επιβλέπουσα)
Αριστείδης Κοντογεώργης	Καθηγητής ΕΚΠΑ	(συνεπιβλέπων)
Αργύριος Φελλούρης	Καθηγητής ΕΜΠ	

Σχολή Εφαρμοσμένων Μαθηματικών και Φυσικών Επιστημών
Εθνικό Μετσόβιο Πολυτεχνείο

Ευχαριστίες

Θα ήθελα να ευχαριστήσω θερμά την κυρία Λαμπροπούλου για την πολύ καλή συνεργασία μας σε όλη τη διάρκεια συγγραφής της παρούσας διπλωματικής παρά το βεβαρημένο πρόγραμμα της. Επίσης θα ήθελα να εκφράσω τις ευχαριστίες μου στον κύριο Κοντογεώργη ο οποίος μου πρότεινε το θέμα και με βοήθησε στη βελτίωση του συνόλου με τις παρατηρήσεις του. Τέλος, θέλω να πω ευχαριστώ στον κύριο Φελλούρη που δέχτηκε να είναι μέλος της επιτροπής και για το χρόνο που αφιέρωσε στην όλη διαδικασία. Για οποιαδήποτε λάθοι, ατέλειες και ελλείμματα περιέχει το κείμενο μοναδικός υπεύθυνος είμαι εγώ.

Περιεχόμενα

Εισαγωγή

Στην εργασία αυτή εξετάζουμε τους κώδικες Reed-Solomon. Ο γράφων προσπάθησε ώστε το θέμα να είναι αυτοτελές και με τις λιγότερο δυνατές προαπαιτούμενες γνώσεις. Έτσι για να φτάσουμε εκεί θα προηγηθεί στο Κεφάλαιο 1 μία σύντομη εισαγωγή στους κώδικες ώστε να καταλάβει ο αναγνώστης το τι είναι ένας κώδικας και πως τον μελετάμε. Στη συνέχεια εξειδικεύουμε στους γραμμικούς κώδικες και ύστερα ακόμα περισσότερο στους πολυωνυμικούς, όπου τέτοιος είναι κι ο κώδικας που μας απασχολεί. Στο Κεφάλαιο 2 αναφέρονται τα απαραίτητα θεωρητικά εργαλεία από το πεδίο της Άλγεβρας που χρειάζονται για τη συνέχεια. Τέλος στο Κεφάλαιο 3 παρουσιάζουμε όλη τη θεωρία των πιο βασικών κωδίκων που ξεκίνησαν από τους κώδικες Reed-Solomon, φτάνοντας μέχρι τους γενικευμένους, πρωτού επιστρέψουμε σε αυτούς για να τους κοιτάξουμε βαθύτερα. Ακολουθούν ορισμένα παραδείγματα και κλείνοντας παρουσιάζουμε τους κώδικες Goppa, που είναι ιδιαιτέρως δημοφιλείς, αποδεικνύοντας ότι κάθε τέτοιος κώδικας είναι υποκώδικας ενός γενικευμένου Reed-Solomon.

Introduction

In this paper, we examine the Reed-Solomon codes. The writer tried for the subject to be self reliant and with the least possible knowledge prerequisites. Chapter 1 is a brief introduction to the codes so that the reader understands what a code is and how we study it. Next, we specify the barcode and then even more in polynomial. Such is also the code that we study. Chapter 2 involves the necessary theoretical tools from the field of Algebra for further analysis. In Chapter 3 we present the theory of the most basic codes initiated by the Reed-Solomon codes, reaching the most general ones, before we go back to them for thorough research. Later we give few examples of such codes. Finally, we present the particularly popular Goppa codes and prove that any such code is a subcode of a generalized Reed-Solomon.

Κεφάλαιο 1

Κώδικες

1.1 Γενικά στοιχεία

Ένας κώδικας μπορεί να πει κάποιος δεν είναι τίποτα άλλο από μία γλώσσα, έτσι σαν κάθε γλώσσα χρειάζεται ένα αλφάβητο. Οποιοδήποτε πεπερασμένο σύνολο από σύμβολα μπορεί να παίξει το ρόλο του αλφαβήτου ενός κώδικα, καθώς για μας όταν ξεκινάμε μια εργασία, αυτά τα σύμβολα στερούνται νοήματος. Το μόνο που μας ενδιαφέρει είναι η διαφορετικότητα τους ως σύμβολα. Έτσι λοιπόν καταλήγουμε στους πρώτους ορισμούς.

[1]Ορισμός

Εστω $A=\{a_1,a_2,\ldots,a_r\}$ ένα τυχαίο μη κενό πεπερασμένο σύνολο από σύμβολα. Το A θα το ονομάζουμε αλφάβητο και τα στοιχεία του χαρακτήρες. Τον αριθμό r θα τον ονομάζουμε πλήθος του A με συμβολισμό $|A|$.

[2]Ορισμός

Κάθε πεπερασμένη ακολουθία $u = (a_{k1},a_{k2},\ldots,a_{kn})$ από στοιχεία του αλφαβήτου ονομάζεται λέξη (ή διάνυσμα) μήκους n. Το μήκος της συμβολίζεται ως $l(u)$.

Το σύνολο των λέξεων του αλφαβήτου συμβολίζεται με A^* . Αυτό προφανώς είναι άπειρο αφού αποτελείται από την ένωση, των αριθμήσιμου πλήθους, ξένων συνόλων A_n . Το καθένα από αυτά ορίζεται να περιέχει αντίστοιχα όλες τις r^n λέξεις μήκους n και μόνο αυτές. Για να είναι το A^* πλήρες κάνουμε την παραδοχή ότι σε αυτό ανήκει και η κενή λέξη, η οποία δεν αποτελείται από κανένα χαρακτήρα κι έχει μήκος μηδέν. Αυτή θα τη συμβολίζουμε με θ όταν την χρειαζόμαστε.

Σε αυτό το σημείο θα ορίσουμε μια μετρική στα σύνολα A_n με σκοπό να μας δείχνει το πόσο διαφέρουν δύο λέξεις ίδιου μήκους.

[3]Ορισμός

Έστω $\chi = (a_{k1},a_{k2},\ldots,a_{kn})$, $y = (\beta_{\lambda1},\beta_{\lambda2},\ldots,\beta_{\lambda n})$ δύο λέξεις του A_n. Ορίζουμε την απεικόνιση $d(\chi,y) = \sum_{i=1}^{n} r_i$, όπου $r_i = 1$ αν στη θέση i τα χ ,y έχουν το ίδιο σύμβολο ενώ διαφορετικά $r_i = 0$.
Προφανώς d: $A_n \times A_n \rightarrow N$. Ο αριθμός αυτός λέγεται *απόσταση Hamming* των λέξεων χ, y .

Για να επαληθεύσουμε ότι η d είναι πράγματι μετρική πρέπει ως γνωστόν να ελεγχθούν οι παρακάτω 3 ιδιότητες :

1. $d(\chi,y) \geq 0$ και $d(\chi,y) = 0$ αν και μόνο αν $\chi = y$ (προφανής).
2. $d(\chi,y) = d(y,\chi)$ (προφανής).
3. $d(\chi,z) \leq d(\chi,y) + d(y,z)$ $\forall$ χ,y,z που ανήκουν στο A_n.

Για την 3. εύκολα βλέπει κάποιος πως αν μια μονάδα προστεθεί στα αριστερά της ισότητας τότε τουλάχιστον μία θα προστεθεί και στα δεξιά. Αυτό διότι αν προστεθεί αριστερά σημαίνει ότι στην εκάστοτε θέση τα *χ,z* διαφέρουν άρα δεν μπορεί στην ίδια θέση το *y* να ταυτίζεται και με τα δύο .

[4]Ορισμός

Έστω *A* ένα αλφάβητο. Κάθε μη κενό υποσύνολο, *C*, του *A**, θα ονομάζεται κώδικας επί του αλφαβήτου *A* και τα στοιχεία του κωδικολέξεις ή κωδικές λέξεις.

Συνήθως το αλφάβητο δεν επιλέγεται τυχαία. Αντιθέτως κοιτάμε τα στοιχεία του να έχουν ιδιότητες οι οποίες θα μας βοηθήσουν να δείξουμε επιθυμητά αποτελέσματα για τον κώδικα μας. Η συνηθέστερη επιλογή είναι κάποιο πεπερασμένο σώμα.

[5]Ορισμός

Ένας κώδικας *C* επί του αλφαβήτου *A* για τον οποίο ισχύει *C* υποσύνολο του A_n θα ονομάζεται *κώδικας σταθερού μήκους*.

Τα πλεονεκτήματα ενός κώδικα σταθερού μήκους είναι ότι μπορούμε να ξέρουμε που ξεκινάει και που τελειώνει μια κωδικολέξη καθώς επίσης ότι έχουμε ήδη μια μετρική για τέτοιους κώδικες που δείχνει πόσο διαφέρει η μία με την άλλη.
(Ωστόσο μπορεί να φτιαχτεί απόσταση παρόμοια με την Hamming και στο σύνολο *A** , όπου αν οι δύο λέξεις έχουν ίδιο μήκος τότε αυτή είναι η Hamming, ενώ αν έχουν διαφορετικό, τότε μετράμε την μικρή με το αρχικό κομμάτι ίδιου μήκους της μεγάλης με τον τρόπο Hamming και ύστερα προσθέτουμε τη διαφορά των μηκών.)

Περιορίζουμε την μελέτη μας από εδώ και κάτω στη περίπτωση που το αλφάβητο μας είναι κάποιο πεπερασμένο σώμα F και ισχύει C υποσύνολο του A_n.

[6]Ορισμός

Έστω a ανήκει A_n, η απόσταση της a από τη μηδενική λέξη 0 = (0,0,…,0) ονομάζεται βάρος αυτής με συμβολισμό w(a).

Προφανώς θα ισχύει ότι $d(\chi,y) = w(\chi - y)$.

1.2 Κωδικοποίηση – Αποκωδικοποίηση

Έστω $S = \{a_1, \dots, a_s\}$ το σύνολο που επιθυμούμε να κωδικοποιήσουμε και *C* το σύνολο του κώδικα μας. Η κωδικοποίηση επιτυγχάνεται με το να ορίσουμε μια 1 - 1 και επί συνάρτηση $f : S \rightarrow C$. Η αποκωδικοποίηση δοθέντος ένος στοιχείου *c* του *C* γίνεται με το να γνωρίζουμε την *f* κι να εφαρμόσουμε την f^{-1} στο c.

Γενικά όταν στέλνεται κάποιο κωδικοποιημένο μήνυμα μπορεί να δημιουργηθεί λάθος κατά τη μεταφορά από τις ατέλειες του τρόπου μετάδοσης. Η ιδέα για να προσδιοριστεί ποιο σύμβολο στάλθηκε είναι να πάρει κάποιος την κωδική λέξη που έφτασε και να δει με ποια από τις λέξεις που ανήκουν στο κώδικα μας έχει την μικρότερη απόσταση Hamming. Με βάση αυτό υποθέτει ότι αυτή είναι και εκείνη που είχε σταλεί και έτσι εφαρμόζει σε αυτή τη f^{-1} για να βρει το σύμβολο του S που θέλει.

Συνήθως δεν θέλουμε να στείλουμε ένα σύμβολο του S τη φορά παρά μια ακολουθία απο αυτά, έτσι ο παραλήπτης αντίστοιχα λαμβάνει μια ακολουθία από κωδικές λέξεις. Έτσι στη πραγματικότητα αυτό που βλέπει ο παραλήπτης είναι μια ακολουθία από σύμβολα του αλφαβήτου του κώδικα μας. Εδώ εφαρμόζεται και το πλεονέκτημα των κωδίκων σταθερού μήκους που αναφέραμε. Παράλληλα όμως διαπιστώνουμε ότι αυτό έρχεται με το αντίβαρο ότι σύμβολα που χρησιμοποιούνται σπάνια αντιστοιχίζονται σε κωδικολέξεις ίδιου μήκους με εκείνα που χρησιμοποιούνται συχνά.

Επιπλέον η συγκεκριμένη μέθοδος για να λειτουργήσει θέτει κάποιους περιορισμούς για το ποιο πρέπει να είναι το υποσύνολο του κώδικα.

[7]Ορισμός

Έστω C ένας κώδικας με τουλάχιστον δύο λέξεις, τότε η ελάχιστη απόσταση $d(C)$ του C είναι η $d(C) = \min\{d(\chi,y) \mid$ για κάθε χ,y που ανήκουν στο C και χ διαφορετικό του $y\}$.

Ένα λάθος e στοιχείο του A_n λέμε ότι ανιχνεύεται από ένα κώδικα C αν η a + e δεν ανήκει στο C για κάθε λέξη a του C. Διαφορετικά δεν θα μπορούμε να γνωρίζουμε αν έχει σταλεί η a ή a + e. Όσον αφορά τους κώδικες λέμε ότι κάποιος από αυτούς, έστω C, ανιχνεύει λ το πλήθος λάθη αν κάθε διάνυσμα λάθους e με βάρος το πολύ λ ανιχνεύεται από εκείνον, ενώ ανιχνεύει ακριβώς λ αν γνωρίζουμε πως ο κώδικας ανιχνεύει λ λάθη και υπάρχει ακόμα κάποιο e_0 με βάρος $\lambda + 1$ που δεν εντοπίζεται.

Ένας κώδικας διορθώνει λ λάθη αν με βάση την μέθοδο της ελάχιστης απόστασης που περιγράψαμε προηγουμένως μπορούμε να βρούμε την a από την a + e για κάθε διάνυσμα λάθους e με βάρος το πολύ λ κι ακριβώς λ αν αντίστοιχα υπάρχει e_0 βάρους $\lambda + 1$ που δε διορθώνεται ενώ ο κώδικας διορθώνει λ λάθη.

[8]Θεώρημα

Ένας κώδικας ανιχνεύει λ το πλήθος λάθη, αν και μόνο αν, $d(C) \geq \lambda + 1$.

Απόδειξη

Αν $d(C) \geq \lambda + 1$ τότε για κάθε διάνυσμα λάθους e με $w(e) \leq \lambda$, η a + e δεν μπορεί να ανήκει στο C, κι αυτό ισχύει για κάθε a του C, αφού διαφορετικά αν υπήρχε κάποιο a_0 ώστε να ανήκει, τότε $d(a_0 + e, a_0) < d(C)$, άτοπο. Η αντίστροφη κατεύθυνση είναι παρόμοια και τώρα προφανής. ∎

[9]Πρόταση

Ένας κώδικας ανιχνεύει ακριβώς λ λάθη, αν και μόνο αν, $d(C) = \lambda + 1$.

Απόδειξη

Από το Θεώρημα [8] ανιχνεύει λ λάθη. Από υπόθεση υπάρχουν κωδικές λέξεις a,b d(a,b) = λ + 1 άρα το διάνυσμα λάθους e = a – b με βάρος w(e) = λ + 1 δεν ανιχνεύεται. Αντίστροφα αφού μπορεί να ανιχνεύσει λ λάθη πρέπει $d(C) \geq \lambda + 1$ όμως αφού δεν μπορεί να ανιχνεύσει λ + 1 πάει να πει από το Θεώρημα[8] πάλι πως $d(C) < \lambda + 2$.

■

[10]Θεώρημα

Ένας κώδικας διορθώνει λ το πλήθος λάθη, αν και μόνο αν, $d(C) \geq 2\lambda + 1$.

Απόδειξη

Έστω ότι $d(C) \geq 2\lambda+1$, τότε για ένα διάνυσμα λάθους e με βάρος το πολύ λ σίγουρα από το Θεώρημα[8] μπορεί να εντοπιστεί. Έστω λοιπόν a η λέξη του κώδικα που στάλθηκε για την οποία αυτή που παραλάβαμε θα ισούται με την a + e. Η a τώρα θα έχει απόσταση το πολύ λ από την a + e, άρα μπορούμε να την βρούμε από την αρχή της ελάχιστης απόστασης. Αυτό γιατί κάθε άλλη λέξη θα απέχει από την a + e απόσταση μεγαλύτερη από λ, ειδάλλως αν χ είναι μια άλλη λέξη με απόσταση το πολύ λ από την a + e, τότε από τριγωνική ανισότητα $d(\chi,a) \leq 2\lambda$, άτοπο.

Αντίστροφα αν ένας κώδικας διορθώνει λ το πλήθος λάθη τότε για δύο τυχαία στοιχεία του χ,y θα ισχύει $d(\chi,y) \geq 2\lambda + 1$. Διαφορετικά έστω a,b με $d(a,b) \leq 2\lambda$, τότε θεωρώ διάνυσμα λάθους e το οποίο ταυτίζεται με το a – b σε κ(w(a – b)/2) το πλήθος τυχαία επιλεγμένες συντεταγμένες και έχει στις υπόλοιπες 0. Η κ(w(a,b)/2) είναι το ακέραιο μέρος του w(a – b)/2 αν αυτό είναι ζυγός ή το ακέραιο μέρος του w(a – b)/2 αυξημένο κατά 1 αν το w(a – b)/2 είναι περιττός. Το κ(w(a,b)/2) προφανώς είναι μικρότερο ή ίσο από το λ. Τότε αν στείλω το b κι παραλειφθεί το b + e ή θα πάρω το a ως απάντηση, γιατί το b + e απέχει από το a μικρότερη απόσταση από το b, που είναι λάθος, ή το b + e θα απέχει την ίδια απόσταση από τα a,b οπότε θα έχουμε αδυναμία αποκωδικοποίησης, άτοπο.

■

[11]Θεώρημα

Ένας κώδικας διορθώνει ακριβώς λ το πλήθος λάθη αν και μόνο αν $d(C) = 2\lambda+1$ ή $d(C) = 2\lambda+2$.

Απόδειξη

Αν ένας κώδικας έχει $d(C) = 2\lambda+1$ ή $d(C) = 2\lambda+2$ τότε από το Θεώρημα[10] θα διορθώνει τουλάχιστον λ λάθη όμως δεν μπορεί να διορθώνει λ + 1, διότι και στις δύο περιπτώσεις $d(C) < 2(\lambda + 1) + 1 = 2\lambda + 3$, άρα από το δεύτερο μέρος της
απόδειξης του Θεωρήματος[10] θα υπάρχει αντιπαράδειγμα. Το αντίστροφο είναι η ίδια συλλογιστική.

■

Μια υποκατηγορία με ιδιαίτερο ενδιαφέρον είναι οι γραμμικοί κώδικες και με αυτούς θα ασχοληθούμε από εδώ και πέρα.

1.3 Γραμμικοί κώδικες

[12]Ορισμός

Ένας σταθερού μήκους *n*, κώδικας *C*, επί ενός αλφαβήτου *F*, όπου το *F* είναι πεπερασμένο σώμα, λέγεται γραμμικός αν είναι υπόχωρος του διανυσματικού χώρου F^n.

Σύμφωνα και με τον παραπάνω ορισμό κάθε γραμμικός κώδικας έχει μια διάσταση *k* και για πλήθος κάποιον αριθμό q^k, όπου *q* το πλήθος των στοιχείων του σώματος *F* (το *q* είναι δύναμη πρώτου, θα δειχθεί στη συνέχεια αυτό). Ορίζουμε ως παραμέτρους ενός γραμμικού κώδικα τα [*n*,*k*,*d*], όπου *n* το μήκος, *k* η διάσταση και *d* η ελάχιστη απόσταση του. Το ότι ο κώδικας μας είναι υπόχωρος μας δίνει μεγάλη ευκολία στην απόδειξη ιδιοτήτων.

[13]Θεώρημα

Έστω *C* ένας γραμμικός κώδικας, η ελάχιστη απόσταση του είναι d(*C*) = min{d(*χ*,0) | *χ* ανήκει στο *C* κι 0 η λέξη (0,0,..,0)}.

Απόδειξη

Προφανώς η λέξη 0 ανήκει στο κώδικα μας. Οπότε η min{d(*χ*,0) | για κάθε *χ* ανήκει στο *C* κι 0 η λέξη (0,0,..,0)}είναι μεγαλύτερη ίση της d(*C*). Αφού d(*χ*,*y*) = w(*χ* – *y*) = d(*χ* – *y*,0) και *χ* – *y* ανήκει στο *C* λόγο γραμμικότητας είναι και μικρότερη ίση. ■

Με το παραπάνω θεώρημα διευκολύνεται κατά πολύ η εύρεση της ελάχιστης απόστασης αφού τότε έχουμε να ελέγξουμε μόνο *M* – 1 αποστάσεις και όχι *M*(*M* – 1)/2 αν έχουμε ένα κώδικα με *M* το πλήθος λέξεις.

Όπως αναφέραμε ήδη οι γραμμικοί κώδικες είναι υπόχωροι άρα έχουν και μία βάση $B = \{b_1, b_2, \ldots, b_k\}$. Εάν τώρα βάλουμε αυτά τα στοιχεία το ένα κάτω από το άλλο δημιουργούμε έναν πίνακα, *G*, μεγέθους (*k* × *n*) με τάξη προφανώς *k*. Αυτός ο πίνακας ονομάζεται *γεννήτορας πίνακας του C*. Για κάθε πίνακα, *R*, (*k* × *k*) τάξης *k*, το γινόμενο R · G είναι κ αυτό γεννήτορας πίνακας του C αφού πάλι οι γραμμές του *R* · *G* θα είναι γραμμικώς ανεξάρτητες. Αυτό ισχύει διότι οι γραμμές των *R*,G είναι γραμμικώς ανεξάρτητες, οπότε αν υπήρχε διάνυσμα γραμμή *χ* (1 × *k*) τ.ω *χ* · *R* · *G* = 0, θα πρέπει (*χ* · *R*) · *G* =0 άρα *χ* · *R* = 0, άρα *χ* = 0. Επομένως αφού θα είναι κι αυτές *k* το πλήθος και παράλληλα στοιχεία του υποχώρου *C*, θα μπορούν και να τον παράγουν αφού αυτός είναι διάστασης *k*. Αντίστροφα αν *G΄* μία άλλη βάση του *C* θα υπάρχει πίνακας, *R*, (*k* × *k*) ώστε *R* · *G΄* = *G* όπου σε κάθε γραμμή, *i*, ο *R* έχει για στοιχεία τους συντελεστές από το *F* που δίνουν το αντίστοιχο διάνυσμα γραμμή *i* του *G*. Προφανώς αυτοί υπάρχουν και είναι μοναδικοί αφού ο *G΄* είναι βάση του υποχώρου μας. Ο *R* θα πρέπει να είναι πάλι τάξης *k* αφού ο *R* · *G΄* είναι, διότι αν ήταν μικρότερης τότε θα υπήρχε διάνυσμα γραμμή μη μηδενικό ώστε *χ* · *R* = 0 κι άρα *χ* · *R* · *G΄* = *χ* · *G* = 0 , άτοπο.

[14]Θεώρημα

Έστω *C* ένας [*n*,*k*,*d*] κώδικας. Τότε υπάρχει βάση αυτού η οποία αν γραφτεί στη μορφή πίνακα, με κατάλληλες μεταθέσεις στηλών αν χρειαστεί, οι πρώτες *k* στήλες του μαζί με τις *k* γραμμές του έχουν τη μορφή I_k του ταυτοτικού τάξης *k*.

Απόδειξη

Ο κώδικας αυτός θα έχει ένα πίνακα γεννήτορα, *G*, (*k* × *n*) τάξης *k* , μπορούμε να μεταθέσουμε τις στήλες ώστε οι πρώτες *k* να είναι γραμμικώς ανεξάρτητες φτιάχνοντας έτσι τον πίνακα *G΄*. Επικεντρώνουμε την προσοχή μας στο πρώτο (*k* × *k*) κομμάτι του πίνακα *G΄*, αυτός ο υποπίνακας μπορεί να θεωρηθεί σαν βάση του F^k κι άρα με γραμμοπράξεις μπορούμε να καταλήξουμε στον ταυτοτικό πίνακα, αυτό μας το εξασφαλίζει το Λήμμα Ανταλλαγής του Steinitz. Με τις αντίστοιχες γραμμοπράξεις εφαρμοσμένες στο *G* γίνεται αυτό που θέλαμε, αφού προφανώς ο καινούριος αυτός πίνακας θα έχει πάλι για γραμμές στοιχεία του υποχώρου C γραμμικώς ανεξάρτητα.

■

[15]Πρόταση

Αν *C* είναι ένας [*n*,*k*,*d*] γραμμικώς κώδικας, τότε $d \leq n - k + 1$.

Απόδειξη

Από το Θεώρημα [14] μπορούμε να υποθέσουμε ότι ο γεννήτορας πίνακας του είναι στη μορφή που υποστηρίζεται εκεί. Τότε κάθε γραμμή που είναι και κωδική λέξη έχει τουλάχιστον *k* – 1 μηδενικά άρα έχει βάρος το πολύ *n* – *k* + 1. Επομένως αφού το 0 είναι κι αυτό πάντα κωδική λέξη ισχύει το ζητούμενο.

■

1.4 Έσωτερικό γινόμενο

Αφού πλέον ασχολούμαστε με γραμμικούς κώδικες θέλουμε να δούμε αν μπορούμε να αναπτύξουμε κάποιου είδους καθετότητα μεταξύ δύο λέξεων ως ένα παραπάνω επίπεδο διαχωρισμού τους. Δηλαδή επιζητάμε κάποια γεωμετρία στις δομές μας. Οπότε θα εισάγουμε την έννοια του εσωτερικού γινομένου.

[16]Ορισμός

Έστω *F* ένα σώμα, *n* φυσικός αριθμός και $\chi = (\chi_1,\chi_2,\ldots,\chi_n)$, $y = (y_1,y_2,\ldots y_n)$ δύο τυχαία στοιχεία του F^n. Το εσωτερικό τους γινόμενο ορίζεται ως $<\chi,y> = \chi_1 y_1 + \ldots + \chi_n y_n$.

θέλουμε να δείξουμε ότι ο παραπάνω ορισμός είναι πράγματι κάποιο είδος εσωτερικού γινομένου οπότε πρέπει να ικανοποιεί τις 3 ιδιότητες

1. $<\chi,y> = <y,\chi>$ για κάθε χ,y του F^n.
2. $<\chi+y,z> = <\chi,z> + <y,z>$ για κάθε χ,y,z του F^n.
3. $<\lambda\chi,y> = \lambda<\chi,y>$ για κάθε λ του *F* και χ,y του F^n.

Η παραπάνω ιδιότητες είναι προφανής από τον Ορισμό [17] και τις ιδιότητες του σώματος.

[17]Ορισμός

1. Δύο στοιχεία χ,y του F^n λέγονται κάθετα αν $<\chi,y> = 0$.
2. Έστω S υποσύνολο του F^n. Το σύνολο $S^{\perp} = \{ \chi$ του $F^n \mid <\chi,s> = 0$ για κάθε s του $S \}$ θα λέγεται ορθογώνιο συμπλήρωμα του S ή δυικός υπόχωρος του S. Η ονομασία δικαιολογείται από κάτω.

[18]Θεώρημα

Το ορθογώνιο συμπλήρωμα $S^{\perp}$ ενός συνόλου S είναι υπόχωρος του F^n και ισχύει $(<S>)^{\perp} = S^{\perp}$, όπου $(<S>)$ ο υπόχωρος που παράγεται από τα στοιχεία του S.

Απόδειξη

Το $S^{\perp}$ προφανώς είναι υπόχωρος αφού αν χ,y ανήκουν στο $S^{\perp}$ και λ ανήκει στο F τότε και $\chi + y$ ανήκει σε αυτό από την ιδιότητα 2 του εσωτερικού γινομένου και το $\lambda\chi$ λόγο της 3. Έστω τώρα χ ανήκει $S^{\perp}$ και y ανήκει στο $(<S>)$ τότε $y = \lambda_1 s_1 + \ldots + \lambda_m s_m$ όπου $\lambda_1,\ldots,\lambda_m$ στοιχεία του F και $s_1,\ldots,s_m$ στοιχεία του S. Άρα από την ιδιότητες 2,3 του εσωτερικού γινομένου το χ ανήκει και στο $(<S>)^{\perp}$, προφανώς ισχύει και το ανάποδο κι άρα και το ζητούμενο. ∎

[19]Πρόταση

Αν C_1 υποσύνολο του C_2 τότε $C_2^{\perp}$ υποσύνολο του $C_1^{\perp}$.

Απόδειξη

Αν χ ανήκει $C_2^{\perp}$ τότε $<\chi,y> = 0$ για κάθε y που ανήκει στο C_2άρα και στο C_1. ∎

[20]Πρόταση

Ένα διάνυσμα είναι κάθετο σε έναν υπόχωρο, αν και μόνο αν, είναι κάθετο στα στοιχεία μιας βάσης του.

Απόδειξη

Λόγο των ιδιοτήτων 2,3 του εσωτερικού γινομένου και του γεγονότος ότι κάθε στοιχείο του υποχώρου είναι γραμμικώς συνδυασμός των στοιχείων της βάσης η πρόταση είναι προφανής. ∎

[21]Ορισμός

Έστω C ένας κώδικας μήκους n από το σώμα F. Αν υπάρχει $(s \times n)$ πίνακας P τ.ω $C = \{$τα στοιχεία c του $F^n \mid c \cdot P^* = 0\}$, όπου P^* ο ανάστροφος του P. Ο P θα ονομάζεται πίνακας ελέγχου ισοτιμίας για τον C ή πιο απλά πίνακας ισοτιμίας.

[22]Πρόταση

Έστω C ένας $[n,k,d]$ γραμμικώς κώδικας με γεννήτορα πίνακα G. Ένας πίνακας P με τάξη $n-k$ είναι πίνακας ισοτιμίας του C, αν και μόνο αν, ισχύει $G \cdot P^* = 0$.

Απόδειξη

Αν ένας πίνακας P είναι έλεγχος ισοτιμίας με τάξη $n-k$ για το C, τότε προφανώς $G \cdot P^* = 0$, αφού κάθε γραμμή του G είναι κωδική λέξη. Αντίστροφα αν $G \cdot P^* = 0$ τότε αυτό μας λέει ότι τα διανύσματα που εκφράζονται από τις γραμμές του P είναι κάθετα στα στοιχεία της βάσης άρα και σε όλον τον C από τη Πρόταση [20]. Οπότε αν c ανήκει C έχουμε $c \cdot P^* = 0$. Ακόμα δεν μπορούν να υπάρχουν στοιχεία χ του F^n εκτός του C τ.ω $\chi \cdot P^* = 0$ (που είναι ισοδύναμο με $P \cdot \chi = 0$). Αυτό διότι η τάξη του P είναι $n-k$, οπότε ο πυρήνας θα πρέπει να έχει διάσταση k. Διότι όπως ξέρουμε η βάση του χώρου του πεδίου ορισμού μπορεί να γραφτεί σαν η βάση του πυρήνα μαζί με στοιχεία που έχουν για εικόνες τα στοιχεία της βάσης του πεδίου τιμών. Το πλήθος της βάσης του πεδίου τιμών όμως θα πρέπει να ταυτίζεται με την τάξη του πίνακα της απεικόνισης. Άρα ο πυρήνας θα έχει διάσταση k κι άρα θα ταυτίζεται με τον υπόχωρο που παράγεται από τον G ο οποίος γνωρίζουμε ήδη πως είναι υποσύνολο του.

▪

Ξέρουμε ότι ο υπόχωρος $C^{\perp}$ ενώς C $[n,k,d]$ κώδικα είναι διάστασης $n-k$, αυτό φαίνεται από την Πρόταση[20] και το γεγονός πως για κάθε χ του F^n , το χ ανήκει στο $C^{\perp}$ αν και μόνο αν $G \cdot \chi = 0$ όπου G γεννήτορας του C. Αυτό γιατί ο G είναι γεννήτορας του C αν και μόνο αν οι γραμμές του είναι διανύσματα που συγκροτούν μια βάση του. Άρα από το τελευταίο μέρος της απόδειξης της πρότασης [22] ο $C^{\perp}$ είναι διάστασης $n-k$.

[23]Πρόταση

Έστω C ένας $[n,k,d]$ γραμμικώς κώδικας και G ένας γεννήτορας πίνακας του, τότε

1. Ο πίνακας G είναι πίνακας ελέγχου για τον $C^{\perp}$.
2. Ο κώδικας $C^{\perp}$ έχει διάσταση $n-k$.
3. $C=(C^{\perp})^{\perp}$.
4. Αν Η γεννήτορας πίνακας του $C^{\perp}$ τότε ο H είναι πίνακας ελέγχου ισοτιμίας για τον C.

Απόδειξη

Οι 1,2 έχουν αποδειχθεί στη συζήτηση που προηγήθηκε. Για τη 3 παρατηρούμε ότι C υποσύνολο του $(C^{\perp})^{\perp}$ κι ότι το $(C^{\perp})^{\perp}$ θα πρέπει να έχει διάσταση k άρα τελικά ισχύει το ζητούμενο. Η 4 προκύπτει από τις 1,3.

▪

[24]Πόρισμα

1. Κάθε ($s \times n$) πίνακας P με στοιχεία από ένα πεπερασμένο σώμα F είναι πίνακας ελέγχου ισοτιμίας ενός γραμμικού κώδικα C.
2. Κάθε ($k \times n$) πίνακας A με στοιχεία από ένα πεπερασμένο σώμα F με τις γραμμές του γραμμικά ανεξάρτητες είναι γεννήτορας πίνακας ενός γραμμικού κώδικα C και πίνακας ελέγχου ισοτιμίας του $C^{\perp}$.
3. Κάθε γραμμικός κώδικας έχει τουλάχιστον ένα πίνακα ελέγχου ισοτιμίας.

Απόδειξη

1. Έστω $C = \{c$ στοιχείο του $F^n \mid c \cdot P^* = 0\}$ προφανώς ο C είναι γραμμικώς κώδικας με τον P πίνακα ισοτιμίας.
2. Προφανές από τα προηγούμενα.
3. Το ίδιο.

■

[25]Πρόταση

Έστω C ένας $[n,k,d]$ γραμμικώς κώδικας με πίνακα ελέγχου ισοτιμίας P. Η ελάχιστη απόσταση d του C είναι ίση με το μικρότερο αριθμό γραμμικά εξαρτημένων στηλών του P.

Απόδειξη

Έστω $p_1,\ldots,p_n$ οι στήλες του P με την ιδιότητα κάθε υποσύνολο αυτών με πλήθος μικρότερο από w να είναι γραμμικώς ανεξάρτητο και ταυτόχρονα να υπάρχουν w το πλήθος στήλες γραμμικώς εξαρτημένες. Τότε υπάρχει ένα διάνυσμα χ ($1 \times n$) με w θέσεις μη μηδενικές και τις υπόλοιπες 0 ώστε $\chi \cdot P^* = 0$. Προφανώς το χ ανήκει στο κώδικα κι έχει βάρος w. Έστω y τυχαίο στοιχείο του κώδικα. Το y δεν γίνεται να έχει λιγότερες από w θέσεις μη μηδενικές διότι θα έπρεπε ο P να έχει ταυτόχρονα κι ένα υποσύνολο γραμμικά εξαρτημένων στηλών με πλήθος μικρότερο από w, άτοπο.

■

1.5 MDS

Συνήθως όταν φτιάχνουμε ένα κώδικα από ένα δεδομένο αλφάβητο ορίζουμε το μήκος του n και την ελάχιστη απόσταση του d που θέλουμε, γιατί από αυτή εξαρτάται πόσα σφάλματα εντοπίζουμε και διορθώνουμε. Ύστερα προσπαθούμε να βρούμε το κώδικα με το μεγαλύτερο πλήθος στοιχείων που ικανοποιεί αυτά τα δεδομένα. Μπορεί όμως αυτή η μέθοδος να μην είναι πολύ αποτελεσματική στη πράξη, είτε γιατί είναι δύσκολο να εντοπιστούν αυτοί οι κώδικες είτε γιατί το πλήθος M των στοιχείων είναι μικρότερο από ότι επιθυμούμε. Τότε ακολουθούμε ένα κάπως αντίστροφο δρόμο. Ορίζουμε το μήκος n του κώδικα και το πλήθος M των στοιχείων που θέλουμε, ύστερα ψάχνουμε να βρούμε από αυτούς τους κώδικες εκείνους που έχουν την μεγαλύτερη ελάχιστη απόσταση D. Στη περίπτωση των γραμμικών κωδίκων (με δεδομένο το αλφάβητο) το να καθορίσεις το πλήθος M είναι ισοδύναμο με το να καθορίσεις τη διάσταση του κώδικα. Όπως έχουμε ήδη δει για ένα γραμμικό κώδικα $[n,k,d]$ ισχύει το φράγμα του *Singleton* δηλαδή $d \leq n - k + 1$, οπότε έχουμε μία

βέλτιστη τιμή που μπορούμε να ψάχνουμε, την $n - k + 1$. Ένα γραμμικό κώδικα με παραμέτρους
$[n,k,n - k + 1]$ τον ονομάζουμε *γραμμικό κώδικα μέγιστης ελάχιστης απόστασης* και τον αναφέρουμε ως MDS. Από τη Πρόταση[26] προκύπτει ένα άμεσο αποτέλεσμα.

[26]Πόρισμα

Έστω C ένας γραμμικός $[n,k,d]$ κώδικας με ένα πίνακα ελέγχου ισοτιμίας P. Ο κώδικας C είναι MDS αν και μόνο αν οποιεσδήποτε $n - k$ το πλήθος στήλες του P είναι γραμμικά ανεξάρτητες.

Απόδειξη

Από την Πρόταση[25] και το γεγονός ότι πάντα έχουμε $d \leq n - k + 1$ προκύπτει το ζητούμενο.

■

Το επόμενο θεώρημα δείχνει μια ισχυρή σύνδεση ανάμεσα στους MDS κώδικες.

[27]Θεώρημα

Ένας γραμμικός κώδικας C επί ενός σώματος F είναι κώδικας MDS, αν και μόνο αν, ο $C^{\perp}$ είναι MDS.

Απόδειξη

Αφού είναι MDS, ο κώδικας C θα έχει παραμέτρους $[n, k, n - k + 1]$, οπότε ο δυικός $C^{\perp}$ θα έχει παραμέτρους $[n, n - k, d]$ αυτό που θέλουμε να δείξουμε είναι ότι
$d = n - (n - k) + 1 = k + 1$. Έστω ότι $d \leq k$ τότε αφού ο κώδικας $C^{\perp}$ είναι γραμμικός θα υπάρχει μία κωδική λέξη c της $C^{\perp}$ για την οποία τα μη μηδενικά της στοιχεία έχουν πλήθος d. Αν H $((n - k) \times n)$ είναι γεννήτορας πίνακας της $C^{\perp}$, από την πρόταση[24] αυτός θα είναι πίνακας ισοτιμίας για τη C, αφού ισχύει $(C^{\perp})^{\perp} = C$. Άρα θα υπάρχει διάνυσμα a του f^{n-k} ώστε $a \cdot H = c$. Πάμε στον H κι αφαιρούμε της d στήλες στις θέσεις που η c έχει μη μηδενικά στοιχεία και στη συνέχεια αν χρειάζεται αφαιρούμε τυχαία κι άλλες $k - d$ στήλες. Οπότε προκύπτει ένας πίνακας P $(n - k) \times (n - k)$ οποίος θα είναι αντιστρέψιμος από το Πόρισμα[26] κι αφού ο Η είναι πίνακας ισοτιμίας για τον C. Τότε ο πολλαπλασιασμός $a \cdot P$ θα πρέπει να δίνει 0 αφού θα έχει σαν αποτέλεσμα ένα διάνυσμα το οποίο θα είναι οι $(n - k)$ εναπομένουσες συντεταγμένες του c όπου μέσα στις k που έχουν αφαιρεθεί βρίσκονται η d μη μηδενικές. Άρα θα πρέπει το a να ισούται με μηδέν οπότε και το c να είναι μηδέν, άτοπο.

■

1.6 Πολυωνυμικοί Κώδικες

Μία από τις σημαντικότερες κατηγορίες γραμμικών κωδίκων είναι οι πολυωνυμικοί με τους οποίους θα ασχοληθούμε και στο υπόλοιπο της εργασίας. Έστω $F_{m-1}[\chi]$ το σύνολο των πολυωνύμων με βαθμό μικρότερο ή ίσο από $m-1$ με συντελεστές από το σώμα F.

[28]Πρόταση

Έστω $\alpha(\chi) = a_0+a_1\chi+\ldots+a_{m-1}\chi^{m-1}$ ανήκει στο $F_{m-1}[\chi]$. Η απεικόνιση $\psi_{F_{m-1}[\chi]}: F_{m-1}[\chi] \rightarrow F^m$ με $\psi_{F_{m-1}[\chi]}(\alpha(\chi))=(\alpha_0,\alpha_1,\ldots,\alpha_{m-1})$ είναι ένας ισομορφισμός διανυσματικών χώρων.

Απόδειξη

Μια βάση του $F_{m-1}[\chi]$ είναι τα στοιχεία $1,\chi\ldots,\chi^{m-1}$ ενώ του F^m είναι τα $(1,0,\ldots,0),(0,1,0,\ldots,0),\ldots,(0,0,\ldots1)$ μέσω της παραπάνω απεικόνισης κάθε στοιχείο της πρώτης βάσης αντιστοιχίζεται σε ένα στοιχείο της άλλης κι αντίστροφα. Επιπλέον η $\psi_{F_{m-1}[\chi]}$ είναι γραμμική κι άρα αποδείχτηκε το ζητούμενο. ∎

Έτσι μπορούμε να ορίσουμε και το βάρος ενός πολυωνύμου ως το βάρος της εικόνας του με την παραπάνω απεικόνιση ψ.

Στη συνέχεια πηγαίνουμε στον $F_k[\chi]$ και διαλέγουμε ένα πολυώνυμο $\gamma(\chi)$ βαθμού k. Για κάθε $\alpha(\chi)$ που ανήκει στο $F_{m-1}[\chi]$ το γινόμενο $\alpha(\chi)\gamma(\chi)$ είναι βαθμού $k+m-1$.

[29]Πρόταση

Η απεικόνιση $\theta: F_{m-1}[\chi] \rightarrow F_{k+m-1}[\chi]$ με $\theta(\alpha(\chi))=\alpha(\chi)\gamma(\chi)$ είναι μία 1-1 γραμμική απεικόνιση. Επομένως η εικόνα $\theta(F_{m-1}[\chi])$ είναι ένας διανυσματικός υπόχωρος διάστασης m του $F_{k+m-1}[\chi]$.

Απόδειξη

Η απεικόνιση είναι γραμμική από τον ορισμό των πράξεων μεταξύ πολυωνύμων κι έχει για πυρήνα το μονοσύνολο$\{0\}$, άρα είναι προφανώς κι 1-1. Οπότε ισχύει η πρόταση αφού οι εικόνες των στοιχείων της βάσης του πεδίου ορισμού θα είναι και βάση για το υπόχωρο του πεδίο τιμών που είναι η εικόνα της συνάρτησης. ∎

[30]Ορισμός

Το σύνολο $C = \{\psi_{F_{k+m-1}[\chi]}(\theta(\alpha(\chi))) = \psi_{F_{k+m-1}[\chi]}(\alpha(\chi)\gamma(\chi)) = (r_0,\ldots,r_{k+m-1}) \mid \alpha(\chi)$ ανήκει $F_{m-1}[\chi]\}$ θα λέγεται πολυωνυμικός κώδικας με πολυώνυμο γεννήτορα το $\gamma(\chi)$.

Το ότι ένας πολυωνυμικός κώδικας είναι ένας γραμμικός κώδικας έπεται από τα προηγούμενα.

Οι παράμετροι ενός πολυωνυμικού κώδικα εξαρτώνται τόσο από το πολυώνυμό γεννήτορα όσο και από το πεδίο ορισμού. Αφού ανάλογα με το ποια θα είναι αυτά τα δύο καθορίζεται το μήκος του κώδικα και η διάσταση του. Η διάσταση θα ταυτίζεται με αυτή του πεδίου ορισμού και το μήκος του θα είναι

αυτό της διάστασης του πεδίου ορισμού αυξημένο κατά το βαθμό του γεννήτορα πολυωνύμου. Αυτά προκύπτουν από τις Προτάσεις [28],[29] και τον τρόπο ορισμού του κώδικα.

Ας δούμε ένα παράδειγμα. Έστω το σώμα Z_5(το γεγονός πως είναι σώμα θα δειχτεί παρακάτω), θα φτιάξουμε ένα πολυωνυμικό κώδικα μήκους 6 με πολυώνυμο γεννήτορα το $\gamma(\chi) = \chi^3 + \chi + 1$. Θέλουμε να βρεθούμε στο χώρο $(Z_5)_5[\chi]$ κι να εφαρμόσουμε εκεί την $\psi_{(Z_5)_5[\chi]}$. Παρατηρούμε ότι ο διανυσματικός χώρος $(Z_5)_2[\chi]$ έχει βάση το σύνολο $\{1,\chi,\chi^2\}$ και πως $1 \cdot \gamma(\chi) = \gamma(\chi)$, $\chi \cdot \gamma(\chi) = \chi^4 + \chi^2 + \chi$, $\chi^2 \cdot \gamma(\chi) = \chi^5 + \chi^3 + \chi^2$. Έτσι έχουμε $\psi_{(Z_5)_5[\chi]}(1 \cdot \gamma(\chi)) = (1,1,0,1,0,0)$, $\psi_{(Z_5)_5[\chi]}(\chi \cdot \gamma(\chi)) = (0,1,1,0,1,0)$, $\psi_{(Z_5)_5[\chi]}(\chi^2 \cdot \gamma(\chi)) = (0,0,1,1,0,1)$ κι οπότε ένας γεννήτορας πίνακας για τον κώδικα μας είναι ο

$$\begin{matrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{matrix}$$

[31]<u>Πρόταση</u>

Η ελάχιστη απόσταση ενός πολυωνυμικού κώδικα είναι ίση με το μικρότερο πλήθος των μη μηδενικών συντελεστών των πολυωνύμων $a(\chi)\gamma(\chi)$, όπου $a(\chi)$ ανήκει στο πεδίο ορισμού του κώδικα και $\gamma(\chi)$ ο γεννήτορας του.

<u>Απόδειξη</u>

Προκύπτει από το ότι ο κώδικας είναι γραμμικός κι από τον τρόπο ορισμού του. ∎

Αν στο πολυώνυμο γεννήτορα ο σταθερός ή/και ο μεγιστοβάθμιος όρος είναι 0 τότε ο πρώτος ή/και ο τελευταίος χαρακτήρας κάθε κωδικολέξης είναι 0 άρα περιττεύει. Οπότε θα θεωρούμε πάντα ότι αυτοί οι όροι είναι διάφοροι του μηδενός.

[32]<u>Πρόταση</u>

Έστω C ένας πολυωνυμικός κώδικας μεγέθους n με γεννήτορα πολυώνυμο $\gamma(\chi) = c_0 + \ldots + c_k\chi^k$. Ένας γεννήτορας πίνακας του C είναι ο

$$\begin{matrix} c_0 & c_1 & \ldots & c_k & 0 & 0 & \ldots & 0 \\ 0 & c_0 & \ldots & c_{k-1} & c_k & 0 & \ldots & 0 \\ . & . & \ldots & . & . & . & \ldots & . \\ . & . & \ldots & . & . & . & \ldots & . \\ . & . & \ldots & . & . & . & \ldots & . \\ 0 & 0 & \ldots & 0 & c_0 & c_1 & \ldots & c_k \end{matrix}$$

Απόδειξη

Η διάσταση του κώδικα είναι προφανώς ίση με το πλήθος των γραμμικώς ανεξάρτητων γραμμών, δηλαδή $n - k$. Κάθε στοιχείο της βάσης από το πεδίο ορισμού του κώδικα είναι ένα πολυώνυμο βαθμού $n - k - 1$. Ο πολλαπλασιασμός κάθε στοιχείου a = $(a_0,..,a_{n-k-1})$ που ανήκει στο F^{n-k} από τα αριστερά με τον πίνακα δίνει τους συντελεστές του γινομένου $a(\chi)\gamma(\chi)$ όπου $a(\chi)$ το πολυώνυμο με συντελεστές το παραπάνω διάνυσμα a και $\gamma(\chi)$ ο γεννήτορας.

■

Στο παράδειγμα πολυωνυμικού κώδικα που δώσαμε βλέπουμε ότι ο πίνακας γεννήτορας που πήραμε είναι στη μορφή που περιγράφει η Πρόταση[32].

[33]Πρόταση

Σε ένα πολυωνυμικό κώδικα ένα διάνυσμα λάθους δεν ανιχνεύεται αν και μόνο αν το αντίστοιχο πολυώνυμο του είναι πολλαπλάσιο του γεννήτορα πολυωνύμου.

Απόδειξη

Προφανής αφού ξέρουμε ότι σε ένα γραμμικό κώδικα ένα διάνυσμα λάθους δεν ανιχνεύεται αν και μόνο αν ανήκει στο κώδικα.

■

[34]Ορισμός

Ένας γραμμικός κώδικας C μήκους n επί του πεπερασμένου σώματος F , θα λέγεται κυκλικός, αν και μόνο αν, για κάθε κωδικολέξη $c = (c_0,\ldots,c_{n-1})$ του C και η $(c_{n-1},c_0,\ldots,c_{n-2})$ ανήκει στο κώδικα.

Στο σημείο αυτό θα σταματήσουμε την εισαγωγή στους κώδικες και θα αναπτύξουμε το αλγεβρικό κομμάτι της εργασίας.

Κεφάλαιο 2

Στοιχεία Άλγεβρας

Στο κεφάλαιο αυτό θα εισάγουμε τα απαραίτητα εργαλεία από το πεδίο της Άλγεβρας. Θα θεωρηθούν γνωστά αρκετά βασικά πράγματα αναφέροντας μόνο τα στοιχεία εκείνα που έχουν άμεση σχέση με το σκοπό μας και βοηθούν στην ουσιαστική κατανόηση του, είτε απευθείας, είτε μέσω των αποδείξεων τους.

[1]Θεώρημα

Κάθε φυσικός αριθμός έχει μοναδική αναπαράσταση ως γινόμενο πρώτων αν εξαιρεθεί η σειρά γραφής των παραγόντων.

Απόδειξη

Το ελάχιστο κοινό πολλαπλάσιο δύο πρώτον αριθμών είναι το γινόμενο τους. Αυτό ισχύει διότι έστω a,b δύο πρώτοι αριθμοί, τότε το ελάχιστο κοινό πολλαπλάσιο τους θα γράφεται στη μορφή γa για κάποιο φυσικό γ. Επίσης ισχύει ότι κάθε άλλο κοινό πολλαπλάσιο τους θα γράφεται ως ($n\gamma$)a για κάποιο φυσικό n. Εάν αυτό δεν ίσχυε θα υπήρχε ένα κοινό πολλαπλάσιο τους δ και φυσικοί m,n(δ) ώστε ($m\gamma$)a < δ = n(δ)a < ((m+1)γ)a άρα και το (n(δ) – ($m\gamma$))a < γa θα ήταν κοινό τους πολλαπλάσιο, άτοπο. Οπότε ($n_0\gamma$)a = ba, κι αφού b πρώτος θα ισχύει b = γ.

Έστω τώρα $a_1, a_2 \ldots, a_n = b_1 b_2 \ldots b_m$ δύο διαφορετικές αναπαραστάσεις με παράγοντες πρώτους αριθμούς ενός φυσικού αριθμού. Τότε ο αριθμός αυτός θα είναι κοινό πολλαπλάσιο των a_1, b_1 . Αν αυτοί είναι ίσοι τους διαγράφουμε από την κάθε μεριά της ισότητας, εάν δεν είναι τότε το $b_1 b_2 \ldots b_m$ πρέπει σύμφωνα με τα προηγούμενα να γράφεται ως $k a_1 b_1$ για κάποιο φυσικό k. Έτσι θα πρέπει να ισχύει $k\, a_1 = b_2 \ldots b_m$ κι ελέγχουμε τώρα αν $a_1 = b_2$, αν όχι τότε συνεχίζουμε αυτή την διαδικασία. Σε κάποια στιγμή θα σταματήσουμε όταν προκύψει ότι $a_1 = b_\lambda$, 2 < λ < m ,ακόμα κι αν $\lambda = m$, τότε τα διαγράφουμε από κάθε πλευρά και συνεχίζουμε με το a_2, η διαδικασία είναι φανερή και το θεώρημα αποδείχτηκε. ∎

[2]Ορισμός

Αβελιανή ονομάζεται μια ομάδα της οποίας η πράξη ικανοποιεί την αντιμεταθετική ιδιότητα.

[3]Ορισμός

Αν υπάρχει $X=\{\chi_1,\ldots,\chi_n\}$ μη κενό υποσύνολο μιας αβελιανής ομάδας G, τ.ω, κάθε στοιχείο a της G γράφεται με μοναδικό τρόπο στη μορφή a = $v_1\chi_{k_1}+\ldots+v_n\,\chi_{k_n}$όπου $v_1,..,v_n$ ακέραιοι και $\chi_1,\ldots,\chi_n$ τα στοιχεία του X, τότε η G λέγεται ελεύθερη αβελιανή ομάδα και το X βάση της.

Το επόμενο σημαντικό θεώρημα όταν μιλάμε για διανυσματικούς χώρους πάνω από κάποιο σώμα, μία δομή που μοιάζει με αυτή της ελεύθερης αβελιανής ομάδας,

συνήθως αποδυκνείεται με το Λήμμα Ανταλλαγής του Steinitz. Όμως εδώ κάθε στοιχείο της βάσης έχει για συντελεστή πάντα κάποιο ακέραιο που δεν διαιρείται σε όλες τις περιπτώσεις οπότε η απόδειξη πρέπει να τροποποιηθεί.

[4]Λήμμα

Για κάθε ελεύθερη αβελιανή ομάδα *G* που έχει πεπερασμένη βάση *X*, υπάρχει φυσικός *r* τ.ω η *G* να είναι ισομορφική με την $Z \times \ldots \times Z$ με *r* παράγοντες, όπου *r* το πλήθος των στοιχείων της *X*.

Απόδειξη

Έστω X=$\{\chi_1,\ldots,\chi_r\}$ τότε για το τυχαίο στοιχείο a της *G* που γράφεται στη μορφή a = $n_1\chi_1+\ldots+n_r\chi_r$ αντιστοιχίζεται στο $(n_1,\ldots,n_r)$ της $Z \times \ldots \times Z$, με αυτή την απεικόνιση το αποτέλεσμα είναι προφανές.

■

[5]Θεώρημα

Αν *G* είναι μια ελεύθερη αβελιανή ομάδα με πεπερασμένη βάση τότε κάθε άλλη βάση της θα έχει τον ίδιο αριθμό στοιχείων.

Απόδειξη

Έστω $\{\chi_1,\ldots,\chi_r\}$ μια βάση για τη *G* ,θεωρούμε το σύνολο 2*G*. Προφανώς αυτή είναι ελεύθερη αβελιανή υποομάδα της *G* με βάση $\{2\chi_1,\ldots,2\chi_r\}$. Σχηματίζω την ομάδα πηλίκο *G*/2*G*. Ορίζουμε για κάθε στοιχείο *b* της *G*/2*G* ως αντιπρόσωπο του, το στοιχείο του *b*, που έχει σε κάθε όρο του αθροίσματος των στοιχείων της βάσης που το παράγουν τον μικρότερο θετικό συντελεστή από τα υπόλοιπα στοιχεία της b. Δηλαδή το a(*b*) = $n_1\chi_1+\ldots+n_r\chi_r$ όπου τα $n_1,\ldots,n_r$ παίρνουν τιμές από το {0,1}. Προφανώς υπάρχουν 2^r τέτοια στοιχεία κι κάθε ένα οφείλει να είναι αντιπρόσωπος σε κάποιο σύμπλοκο και ταυτόχρονα κάθε σύμπλοκο έχει κι από ένα μόνο τέτοιο στοιχείο. Αυτό γιατί δοθέντος ενός συμπλόκου *b* της *G*/2*G* κι ενός τυχαίου στοιχείο γ αυτού μπορώ να φτάσω στο a(b) μειώνοντας μία συντεταγμένη τη φορά με απανωτές αφαιρέσεις του $2\chi i$ το οποίο ανήκει για κάθε *i* στη 2*G*. Άρα r = log2(|*G*/2*G*|) δηλαδή σταθερό που συνεπάγεται ότι κάθε πεπερασμένη βάση έχει το ίδιο πλήθος στοιχείων.

Έστω τώρα ότι η *G* έχει μια άπειρη βάση και μια πεπερασμένη. Τότε κάθε στοιχείο της πεπερασμένης γράφεται σαν κατάλληλο άθροισμα από πεπερασμένα στο πλήθος στοιχεία της μεγάλης. Οπότε για να κατασκευασθούν όλα τα στοιχεία της μικρής βάσης αρκούν πεπερασμένα της μεγάλης. Διαλέγουμε τώρα ένα στοιχείο από την άπειρη βάση που δεν έχει χρησιμοποιηθεί στην κατασκευή των στοιχείων της μικρής, αυτό θα έχει δύο αναπαραστάσεις, μία ως ο εαυτός του και μία ως κατάλληλο άθροισμα από τα στοιχεία της μεγάλης βάσης που χρησιμοποιήθηκαν για την κατασκευή της μικρής, άτοπο.

■

[6]Ορισμός

Αν μια ελεύθερη αβελιανή ομάδα έχει πεπερασμένη βάση, το πλήθος των στοιχείων της βάσης λέγεται διάσταση της ομάδας.

[7]Θεώρημα

Αν X=$\{\chi_1,..,\chi_n\}$ μια βάση μιας ελεύθερης αβελιανής ομάδας G τότε και η Y=$\{\chi_1,..,\chi_{j-1}, \chi_j + t\chi_i, \chi_{j+1},\ldots,\chi_n\}$ είναι βάση της G.

Απόδειξη

Κάθε στοιχείο a της G μπορεί να γραφεί σαν κατάλληλο άθροισμα στοιχείων της Y. Το διαπιστώνουμε βλέποντας ότι αν στη γραφή του a δεν χρησιμοποιείται το χ_j τότε είναι το ίδιο με το άθροισμα των στοιχείων της X. Αντιθέτως αν χρησιμοποιείται τότε γράφουμε το άθροισμα των στοιχείων της X που δίνει το a κι προσθέτουμε κι αφαιρούμε το $v_j t\chi_i$ όπου v_j ο συντελεστής του χ_j. Προφανώς κάθε στοιχείο έχει πάλι μοναδική γραφή από αθροίσματα στοιχείων της Y αφού στην τελική μπορούμε να το δούμε σαν αθροίσματα των στοιχείων της αρχικής μας βάσης.

■

[8]Θεώρημα

Έστω G μια μη μηδενική ελεύθερη αβελιανή ομάδα διάστασης n και K μια μη μηδενική υποομάδα της. Τότε η K είναι ελεύθερη αβελιανή ομάδα διάστασης $s \leq n$. Ακόμη υπάρχει μια βάση $\{\chi_1,\ldots,\chi_n\}$ της G και θετικοί ακέραιοι $d_1,\ldots,d_s$ ώστε το$\{d_1\chi_1,\ldots,d_s\chi_s\}$να είναι βάση της K.

Απόδειξη

Θα αποδείξουμε ότι υπάρχει μία βάση για την K στη ζητούμενη μορφή. Έστω Y=$\{y_1,\ldots,y_n\}$ μία τυχαία βάση της G. Κάθε μη μηδενικό στοιχείο της K γράφεται στη μορφή $k_1y_1+\ldots+k_ny_n$ όπου κάποια από τα k_i είναι μη μηδενικά. Μπορούμε να αντιστοιχίσουμε σε κάθε βάση Y τον αριθμό ο οποίος θα είναι η μικρότερη τιμή των συντελεστών $|k_i|$ καθώς τα μη μηδενικά στοιχεία της K γράφονται με τη βοήθεια της Y. Διαλέγουμε μια βάση $Z = \{z_1,\ldots,z_n\}$ της οποίας αυτός ο αριθμός είναι ελάχιστος ανάμεσα σε όλες τις βάσεις κι έστω ότι είναι ο d_1. Αριθμώντας ξανά αν είναι απαραίτητο θα υπάρχει στοιχείο w_1 της K ώστε $w_1 = d_1z_1+\ldots+k_nz_n$, τότε ο w1 γράφεται στη μορφή $w_1 = d_1(z_1 + q_2z_2 +\ldots+ q_nz_n) + r_2z_2+\ldots+ r_nz_n$ όπου q_i,r_i είναι το πηλίκο και το υπόλοιπο αντίστοιχα των k_i με το d_1. Έστω τώρα χ_1 το $z_1 + q_2z_2 +\ldots+ q_nz_n$ τότε από το Θεώρημα [6] επαγωγικά και η $\{\chi_1,z_2,\ldots,z_n)$ είναι βάση της G, άρα από τον τρόπο ορισμού του d_1 θα πρέπει $r_2,\ldots,r_n$ να ισούνται με το 0. Για τον ίδιο λόγο αν γράψουμε το τυχαίο στοιχείο της K με τη βοήθεια της$\{\chi_1,z_2,\ldots,z_n\}$ ως $h_1\chi_1 + k_2z_2 +\ldots+ k_nz_n$ θα πρέπει το h να είναι πολλαπλάσιο του d1, διότι διαφορετικά αφού το $d_1\chi_1$ ανήκει στη K, αν το αφαιρούσαμε κατάλληλο αριθμό φορών θα παραμέναμε μέσα στην K κι θα παίρναμε ένα συντελεστή μικρότερο του d_1, άτοπο. Πηγαίνουμε τώρα σε όλα τα υποσύνολα του G μεγέθους $n - 1$, έστω Γ, στα οποία αν τους προσθέσεις το χ_1 θα γίνουν βάση της G. Αντιστοιχίζουμε σε καθε ένα από αυτά τον μικρότερο κατά απόλυτη τιμή συντελεστή που έχει κάποιο στοιχείο του εκάστοτε συνόλου Γ όταν περιγράφει κάποιο μη μηδενικό στοιχείο του K. Διαλέγουμε ένα υποσύνολο που έχει ελάχιστο τέτοιο αντιστοιχισμένο αριθμό ανάμεσα στα Γ,έστω Γ', κι επαναλαμβάνουμε τη διαδικασία για να βρούμε το χ_2 και το d_2. Δηλαδή αν $\Gamma' = \{\gamma_1,\ldots,\gamma_{n-1}\}$είναι ένα τέτοιο σύνολο, τότε κάθε στοιχείο του K θα γράφεται με τη βοήθεια του Γ U $\{\chi_1\}$ ως $\lambda_1d_1\chi_1 + k_1\gamma_1 +\ldots+ k_{n-1}\gamma_{n-1}$

οπότε θα πρέπει και το $k_1\gamma_1$ +…+ $k_{n-1}\gamma_{n-1}$ να ανήκει στο K. Άρα από το κριτήριο επιλογής του Γ΄ θα υπάρχει w_2 που ανήκει στο K με $w_2 = d_2\gamma_1$ + …+ $k_{n-1}\gamma_{n-1}$ όπου d_2 ο θετικός συντελεστής με τη καινούρια μικρότερη απόλυτη τιμή που ζητάμε κ.ο.κ.. Ύστερα πηγαίνουμε σε όλα τα υποσύνολα του *G* μεγέθους $n-2$ στα οποία αν τους προσθέσεις το $\{\chi_1,\chi_2\}$γίνονται βάση κι κάνουμε την ίδια διαδικασία. .

■

Θεωρείται γνωστό τι είναι η πεπερασμένα παραγόμενη ομάδα.

[9]Θεώρημα

Κάθε πεπερασμένα παραγόμενη αβελιανή ομάδα είναι ισόμορφη με μια ομάδα της μορφής $Z_{d_1} \times Z_{d_2} \times \ldots \times Z_{d_r} \times Z \times \ldots \times Z$.

Απόδειξη

Έστω *G* μια πεπερασμένα παραγώμενη αβελιανή ομάδα κι $\{a_1,\ldots,a_n\}$ ένα σύνολο γεννητόρων της. Τότε η απεικόνιση *f*: *Z* × *Z*… *Z*(*n* φορές) → *G* όπου $f(h_1,\ldots,h_n) = h_1a_1 + \ldots + h_na_n$ είναι προφανώς ομομορφισμός και επί. Άρα η *G* θα είναι ισομορφική με την ομάδα πηλίκο που δημιουργεί ο πυρήνας της απεικόνισης κι άρα από το Θεώρημα[7] και τη διαδικασία που περιγράφτηκε στην απόδειξη του Θεωρήματος[4] προκύπτει το ζητούμενο.

■

[10]Θεώρημα

Η ομάδα $\prod_{i=1}^{r} Z_{m_i}$ είναι κυκλική και ισόμορφη με την $Z_{m_1\ldots m_r}$ αν και μόνο αν οι $m_1,\ldots,m_r$ είναι πρώτοι ανά δύο.

Απόδειξη

Αν οι αριθμοί είναι πρώτοι ανά δύο τότε το ελάχιστο κοινό πολλαπλάσιο τους είναι το $m_1\ldots m_r$ το οποίο προκύπτει από το Θεώρημα[1], οπότε πηγαίνοντας στην $\prod_{i=1}^{r} Z_{m_i}$ κι αντιστοιχίζοντας το (1,…,1) στο 1 κι όλη την κυκλική ομάδα που παράγεται απ' αυτό με τον φυσιολογικό τρόπο θα πάρουμε τον ισομορφισμό αφού για να είναι 0 όλες οι συντεταγμένες μαζί για πρώτη φορά θα πρέπει να φτάσουμε στο ελάχιστο κοινό πολλαπλάσιο των m_i. Αντίστροφα αν οι δύο αυτές ομάδες ήταν ισομορφικές αλλά δεν ήταν οι αριθμοί πρώτοι μεταξύ τους θα πρέπει το ελάχιστο κοινό τους πολλαπλάσιο να είναι μικρότερο του $m_1\ldots m_r$, οπότε πηγαίνοντας στην συνάρτηση με την οποία είχαν καταστεί ισομορφικές βλέπουμε τον γεννήτορα 1 του $Z_{m_1\ldots m_r}$ και παρατηρούμε ότι με απανωτές προσθέσεις φτάνοντας στο ελάχιστο κοινό πολλαπλάσιο, αυτό θα πρέπει να αντιστοιχίζεται λόγο του ισομρφισμού στο 0, άτοπο αφού τότε ο πυρήνας δε θα είναι μονοσύνολο.

■

[11]Ορισμός

Ένα σώμα Ε λέγεται επέκταση σώματος ενός σώματος *F* αν $F \leq E$.

[12]Ορισμός

Ένα στοιχείο a μιας επέκτασης E ενώς σώματος F λέγεται αλγεβρικό πάνω από το F αν υπάρχει κάποιο μη μηδενικό πολυώνυμο $f(\chi)$ του $F[\chi]$ ώστε $f(a) = 0$. Σε αντίθετη περίπτωση το a λέγεται υπερβατικό πάνω από το F.

[13]Ορισμός

Μια επέκταση E ενός σώματος F λέγεται αλγεβρική επέκταση του F ,αν και μόνο αν, κάθε στοιχείο του E είναι αλγεβρικό πάνω από το F.

[14]Ορισμός

Αν μια επέκταση E ενός σώματος F έχει πεπερασμένη διάσταση n ως διανυσματικός χώρος πάνω από το F, τότε το E λέγεται πεπερασμένη επέκταση βαθμού n πάνω από το F, και το n συμβολίζεται ως $[E:F]$.

[15]Ορισμός

Αν E είναι μία αλγεβρική επέκταση ενός σώματος F και a ανήκει στο E, τότε $F(E)(a)$ συμβολίζεται το ελάχιστο υπόσωμα του E που περιέχει το F και το a.

[16]Θεώρημα

Κάθε σώμα έχει μία αλγεβρική θήκη, δηλαδή μία αλγεβρική επέκταση που είναι αλγεβρικά κλειστή.

Απόδειξη

Η απόδειξη δεν είναι δύσκολη είναι όμως μεγάλη και παραλείπεται, μπορεί κάποιος να τη δει από κάποιο βιβλίο όπως π.χ του Fraleigh.

■

Στα επόμενα κάθε επέκταση κάποιου σώματος θα θεωρούμε ότι συμβαίνει μέσα σε μία σταθερή αλγεβρική του θήκη κι άρα αντί για $F(E)(a)$ θα γράφουμε σκέτο $F(a)$.

[17]Θεώρημα

Έστω E μια πεπερασμένη επέκταση βαθμού n πάνω από ένα πεπερασμένο σώμα F. Αν το F έχει q στοιχεία τότε η E έχει q^n στοιχεία.

Απόδειξη

Έστω $A=\{a_1,\ldots,a_n\}$ μια βάση του E πάνω από το σώμα F, τότε κάθε στοιχείο β του E γράφεται μοναδικά στη μορφή $\beta = k_1a_1 +\ldots+ k_na_n$ όπου τα k_i ανήκουν στο F για κάθε i. Αντίστροφα κάθε τέτοιας μορφής άθροισμα αντιστοιχεί σε ένα μοναδικό στοιχείο του E, άρα έπεται το ζητούμενο.

■

[18]Ορισμός

Αν για κάποιο δακτύλιο R υπάρχει ένας θετικός ακέραιος n τ.ω για κάθε a που ανήκει στο R, ισχύει, $n \cdot a = 0$, τότε ο μικρότερος από αυτούς λέγεται χαρακτηριστική του σώματος. Αν δεν υπάρχει κανένας τέτοιος φυσικός αριθμός λέγεται ότι ο R έχει χαρακτηριστική 0.

[19]Θεώρημα

Αν R είναι ένας δακτύλιος με μοναδιαίο στοιχείο το 1, τότε ο R είναι χαρακτηριστικής $n > 0$ αν και μόνο αν n είναι ο μικρότερος θετικός ακέραιος για τον οποίο $n \cdot 1 = 0$.

Απόδειξη

Από τον Ορισμό[11] αν n είναι χαρακτηριστική του δακτυλίου τότε $n \cdot 1 = 0$. Αντιστρόφως αν m είναι ένας θετικός ακέραιος για τον οποίο $m \cdot 1 = 0$ τότε για κάθε a που ανήκει στο R ισχύει $m \cdot a = (1 +\ldots+ 1)a = 0a = 0$, όπου προστέθηκαν στη παρένθεση m μονάδες. Από τα παραπάνω προκύπτει το αποτέλεσμα.

■

[20]Θεώρημα

Αν G είναι μια ομάδα και a στοιχείο αυτής τότε το $H =\{a^n| \ n$ ακέραιος$\}$ είναι κυκλική υποομάδα και μάλιστα η ελάχιστη υποομάδα της G που περιέχει το a.

Απόδειξη

Προφανές.

■

[21]Ορισμός

Η υποομάδα *H* του Θεωρήματος [20] ονομάζεται η υποομάδα της *G* που παράγεται από το a και συμβολίζεται <a>.

[22]Ορισμός

Αν a και *b* είναι δύο μη μηδενικά στοιχεία ενός δακτυλίου *R* τ.ω a*b* = 0, τότε τα a,*b* λέγονται διαιρέτες του 0 και συγκεκριμένα το a αριστερός διαιρέτης του 0 και ο *b* δεξιός.

[23]Θεώρημα

Στον δακτύλιο Z_n οι διαιρέτες του 0 (δεν υπάρχει διάκριση σε αριστερούς και δεξιούς αφού η πράξη του πολλαπλασιασμού είναι αντιμεταθετική εκεί) είναι ακριβώς εκείνα τα στοιχεία που δεν είναι πρώτα προς των *n*.

Απόδειξη

Έστω *m* ανήκει στον Z_n, *m* διαφορετικό του 0 με *d* μέγιστο κοινό διαιρέτη με το *n* διαφορετικό του 1. Τότε *m*(*n*/*d*) = (*m*/*d*)*n* = 0. Αντίστροφα αν κάθε στοιχείο του Z_n είναι πρώτο προς το *n* τότε δεν γίνεται δύο στοιχεία του Z_n να δίνουν κάποιο πολλαπλάσιο του *n* για να πάρουμε 0 αφού αν γινόταν κάτι τέτοιο από την μοναδική αναπαράσταση φυσικού αριθμού ως γινόμενο πρώτον θα καταλήγαμε σε άτοπο.

■

Από το παραπάνω Θεώρημα βλέπουμε ότι σώματα είναι μόνο οι δακτύλιοι Z_n, όπου *n* πρώτος. Τα σώματα αυτά ονομάζονται *πρώτα σώματα.*

[24]Πόρισμα

Για κάθε σώμα *F* χαρακτηριστικής διαφορετικής του μηδενός, έστω *q*, θα πρέπει *q* πρώτος.

Απόδειξη

Κάθε σώμα περιέχει ένα αντιμεταθετικό δακτύλιο με μοναδιαίο στοιχείο, αυτό που παράγεται μέσω της προσθετικής πράξης από τη μονάδα του. Αυτός είναι ισομορφικός με το Z_q. Άρα αν το q δεν ήταν πρώτος, το *F* θα είχε διαιρέτες του μηδενός, άτοπο.

■

[25]Πόρισμα

Αν E είναι ένα πεπερασμένο σώμα χαρακτηριστικής p τότε το E περιέχει p^n στοιχεία για κάποιον φυσικό n.

Απόδειξη

Κάθε πεπερασμένο σώμα E είναι πεπερασμένη επέκταση ενός πρώτου σώματος ισόμορφου με το Z_p, συγκεκριμένα της υποομάδας που παράγεται μέσω της προσθετικής πράξης από τη μονάδα του, όπου p η χαρακτηριστική του E. Από το Θεώρημα [17] προκύπτει αυτό που θέλουμε.

■

[26]Θεώρημα

Έστω ένα σώμα E με p^n στοιχεία που περιέχεται σε μία αλγεβρική θήκη του Z_p. Τα στοιχεία του E είναι ακριβώς οι ρίζες του πολυωνύμου $\chi^{p^n} - \chi$ στην αλγεβρική θήκη.

Απόδειξη

Το σύνολο E^* των μη μηδενικών στοιχείων του E είναι μία ομάδα τάξης $p^n - 1$ με την πράξη του πολλαπλασιασμού του σώματος και με ουδέτερο στοιχείο τη μονάδα. Έτσι από το Θ.Lagrange για κάθε στοιχείο a του E ισχύει $a^{p^n-1} = 1$ οπότε κάθε στοιχείο του E είναι ρίζα του $\chi^{p^n} - \chi$ κι αφού αυτό μπορεί να έχει το πολύ p^n ρίζες έχουμε τελειώσει.

■

Το παραπάνω θεώρημα ισχύει για κάθε σώμα E χαρακτηριστικής p, όπου το ρόλο του Z_p το παίζει το σώμα που παράγεται από τη μονάδα. Η απόδειξη είναι η ίδια μόνο με αλλαγή των ονομάτων, πράγμα που είναι προφανές κι από τον ισομορφισμό μεταξύ αυτών των δύο σωμάτων.

[27]Θεώρημα

Αν G είναι μια πεπερασμένη πολλαπλασιαστική υποομάδα της πολλαπλασιαστικής ομάδας $<F^*, \cdot>$ των μη μηδενικών στοιχείων ενός σώματος F, τότε η G είναι κυκλική.

Απόδειξη

Από τα Θεωρήματα [8],[9] η G ως πεπερασμένα παραγώμενη (αφού είναι πεπερασμένη) αβελιανή ομάδα είναι ισόμορφη με ένα ευθύ γινόμενο $Z_{d_1} \times Z_{d_2} \times \ldots \times Z_{d_r}$. Έστω m το ελάχιστο κοινό πολλαπλάσιο των d_i. Αν a_i ανήκει στο Z_{d_i} ισχύει ${a_i}^m = 1$ οπότε για κάθε στοιχείο b του γινόμενου ισχύει $b^m = 1$ κι

άρα λόγο του ισομορφισμού κι για κάθε στοιχείο γ του G ισχύει $\gamma^m = 1$ οπότε κάθε ένα από τα $d_1 \cdot \ldots \cdot d_r$ στοιχεία του G είναι ρίζα του $\chi^m - 1$ το οποίο μπορεί να έχει το πολύ m ρίζες. Με δεδομένο ότι $d_1 d_2 \ldots d_r \geq$ m καταλήγουμε πως οι $d_1, d_2, \ldots, d_r$ είναι πρώτοι ανα δυό κι άρα από το Θεώρημα[9] η G είναι ισομορφική με τη $Z_{d_1 \ldots d_r}$ κι άρα κυκλική.

■

[28]Θεώρημα

Η πολλαπλασιαστική ομάδα όλων των μη μηδενικών στοιχείων ενός πεπερασμένου σώματος είναι κυκλική.

Απόδειξη

Άμεση από το Θεώρημα.[26].

■

[29]Θεώρημα

Κάθε πεπερασμένη επέκταση E ενός πεπερασμένου σώματος F είναι απλή επέκταση του F.

Απόδειξη

Έστω a γεννήτορας της κυκλικής ομάδας E^* των μη μηδενικών στοιχείων του E. Άμεσα ισχύει $E = F(a)$.

▪

[30]Θεώρημα

Αν F είναι ένα πεπερασμένο σώμα χαρακτηριστικής p με αλγεβρική θήκη F'', τότε το $\chi^{p^n} - \chi$ έχει p^n διακεκριμένες ρίζες.

Απόδειξη

Προφανώς το 0 είναι ρίζα του πολυωνύμου οπότε αυτό παραγοντοποιείται στο χ ($\chi^{p^n-1} - 1$). Είναι φανερό πως οι υπόλοιπες ρίζες θα είναι του $f(\chi) = \chi^{p^n-1} - 1$. Έστω a μία τέτοια ρίζα. Τότε λόγο του γεγονότος ότι $a^{p^n-1} = 1$ ισχύει $f(\chi) = (\chi - a)(\chi^{p^n-2} + \chi^{p^n-3}a + \ldots + a^{p^n-2})$. Τώρα το $\chi^{p^n-2} + \chi^{p^n-3}a + \ldots + a^{p^n-2}$ έχει $p^n - 1$ προσθετέους και για $\chi = a$ δίνει $[(p^n - 1) \cdot 1]\, a^{p^n-2} = -1/a$, το οποίο είναι διαφορετικό του μηδενός.

■

[31]Θεώρημα

Για κάθε δύναμη πρώτου p^n υπάρχει ένα πεπερασμένο σώμα με GF(p^n) με p^n στοιχεία.

Απόδειξη

Έστω $Z_p{}''$μία αλγεβρική θήκη του Z_p και *K* το υποσύνολο του $Z_p{}''$ (το οποίο είναι προφανώς χαρακτηριστικής *p*) που αποτελείται από όλες τις ρίζες του $\chi^{p^n} - \chi$ στο Z_p. Τότε για κάθε a,b του *K* ισχύουν οι ισότητες $(a \pm b)^{p^n} = a^{p^n} \pm b^{p^n} = a \pm b$. Αυτό λόγο του διωνυμικού τύπου κι επειδή κάθε συντελεστής εκτός των a^{p^n}, b^{p^n} θα είναι πολλαπλάσιο του p αφού αυτό είναι πρώτος. Άρα λόγω του ότι p είναι και η χαρακτηριστική τιμή του σώματος οι συντελεστές θα ισούνται με το 0. Επίσης ισχύει προφανώς $(ab)^{p^n} = a^{p^n} b^{p^n}$ άρα το *K* είναι κλειστό σώμα αφού το 0 και το 1 ανήκουν σε αυτό και $(1/a)^{p^n} = 1/a$ για a που ανήκει στο *K*. Επομένως το *K* περιέχει και το Z_p αφού αυτό παράγεται με πρόσθεση από το 1. Το $\chi^{p^n} - \chi$ από το Θεώρημα [30] έχει p^n διακεκριμένες ρίζες άρα τελειώσαμε. ∎

[32]Ορισμός

Μονικό πολυώνυμο ενός στοιχείου a πάνω από ένα σώμα *F* λέγεται, αν υπάρχει, το ελάχιστο από άποψη βαθμού πολυώνυμο με συντελεστές από το *F* που έχει για ρίζα το a με συντελεστή του μεγιστοβάθμιου όρου του τη μονάδα. Συμβολίζεται irr(a,*F*).

[33]Πόρισμα

Αν *F* είναι οποιοδήποτε πεπερασμένο σώμα, τότε για κάθε θετικό ακέραιο *n*, υπάρχει ένα ανάγωγο πολυώνυμο στον *F*[χ] βαθμού *n*.

Απόδειξη

Έστω ότι το *F* έχει q = p^r στοιχεία, όπου *p* είναι η χαρακτηριστική του *F*. Όπως έχουμε πει το σώμα που παράγεται από διαδοχικές προσθέσεις της μονάδας είναι ισόμορφο με το Z_p με το φυσικό ισομορφισμό , δλδ το 1+1 = 2 κοκ , άρα η απόδειξη του Θεωρήματος [31] μπορεί να γίνει χωρίς καμία αλλαγή και για την αλγεβρική θήκη F΄΄ του *F*. Οπότε υπάρχει υπόσωμα *K* του *F΄΄* το οποίο αποτελείται ακριβώς από όλες τις ρίζες του $\chi^{p^{rn}} - \chi$ και οι οποίες από το Θεώρημα [30] είναι p^{rn} . Κάθε στοιχείο του *F* προφανώς από το Θ.Lagrange είναι ρίζα του $\chi^{p^r} - \chi$, σκοπός μας είναι να δείξουμε ότι είναι και στοιχεία του K. Έστω a ανήκει στο F, για αυτό ισχύει $a^{p^r} = a$, υψώνουμε κάθε μέρος της ισότητας στο p^r κι έχουμε $a^{(p^r)^{p^r}} = a^{p^r}$ το

οποίο είναι ισοδύναμο με $a^{p^{2r}} = a^{p^r} = a$. Αν το κάνουμε αυτό άλλες $n-2$ φορές φτάνουμε στο $a^{p^{nr}} = a$ και τελειώσαμε. Έτσι μπορούμε να δούμε το K σαν $K = F(b)$ για κάποιο b του K. Δηλαδή το ανάγωγο πολυώνυμο το οποίο είναι το μονικό του b πάνω από το F πρέπει να έχει βαθμό n.

▪

Το επόμενο θεώρημα μας δείχνει πως ουσιαστικά υπάρχει όλα τα πεπερασμένα σώματα με την ίδια χαρακτηριστική ταυτίζονται εκτός από το όνομα των στοιχείων τους. Αφού κάθε πεπερασμένο σώμα έχει μια χαρακτηριστική τιμή ουσιαστικά λέει πως ένα σώμα προσδιορίζεται πλήρως από την χαρακτηριστική του τιμή.

[34]Θεώρημα

Έστω E μια αλγεβρική θήκη ενός σώματος F. Έστω σ ένας ισομορφισμός του F επί ενός σώματος F'.Έστω E' μια αλγεβρική θήκη του F'. Τότε μπορούμε να επεκτείνουμε τον σ σε έναν ισομορφισμό τ του E επί ενός υποσώματος του E' ώστε $\tau(a) = \sigma(a)$ για κάθε a που ανήκει στο F.

Απόδειξη

Το θεώρημα αποδεικνύεται με βάση το Λήμμα Zorn. Θεωρούμε όλα τα ζεύγη (L,λ), όπου L είναι σώμα τ.ω $F \leq L \leq E$ και λ ισομορφισμός του L με ένα υπόσωμα του E', ώστε $\lambda(a) = \sigma(a)$ για κάθε a που ανήκει στο F. Το σύνολο S αυτών των ζευγών είναι μη κενό αφού το (F,σ) ανήκει εκεί. Ορίζουμε και μια μερική διάταξη στο S ως εξής, $(L_1,\lambda_1) \leq (L_2,\lambda_2)$ αν και μόνο αν $L_1 \leq L_2$ και $\lambda_1(a) = \lambda_2(a)$ για κάθε a που ανήκει στο L_1. Είναι τετριμμένο να ελεγχθεί ότι οι υποθέσεις του Zorn ικανοποιούνται. Έστω λοιπόν (K,τ) ένα μεγιστικό στοιχείο εκεί, αν $K < E$ τότε θα υπάρχει a του E που δεν ανήκει στο K, όμως αφού το E είναι αλγεβρική θήκη και του K αφού $F \leq K$ θα υπάρχει το irr(K,a). Έστω ψ(a) ο κανονικός ισομορφισμός ψ(a): $K[\chi]/\langle \text{irr}(K,a)\rangle \rightarrow K(a)$. Έστω $\tau(K)=K'$ τότε θεωρούμε τον φυσικό ισομορφισμό $\Gamma : K[\chi] \rightarrow K'[\chi]$ όπου το πολυώνυμο του $K[\chi]$ αντιστοιχίζεται σε αυτό που έχει για συντελεστές την ισομορφική εικόνα των συντελεστών του πρώτου αντίστοιχα σε κάθε θέση. Το Γ (irr(K,a)) προφανώς θα είναι ανάγωγο στο K' και θα έχει μια ρίζα στο E', έστω a΄. Θεωρούμε τώρα τον αντίστοιχο κανονικό ισομορφισμό ψ(a΄): $K'[\chi]/\langle \Gamma(\text{irr}(K,a))\rangle \rightarrow K'(a')$ και τέλος τον φυσικό ισομορφισμό τ΄΄: $K[\chi]/\langle \text{irr}(K,a)\rangle \rightarrow K'[\chi]/\langle \Gamma(\text{irr}(K,a))\rangle$ που επάγεται από τον Γ. Τότε η απεικόνιση $[\psi(a')\tau''\psi(a)^{-1}]$: K(a) → K΄(a΄) είναι ισομορφισμός και επομένως το ζεύγος $(K(a), [\psi(a')\tau''\psi(a)^{-1}])$ ανήκει στο S, άτοπο.

▪

Έστω ένα σώμα F, γι αυτό ορίζεται μία συνάρτηση det από το σύνολο των τετραγωνικών πινάκων, όλων των μεγεθών, στο F η οποίο προσδιορίζεται μοναδικά από τις ακόλουθες τρεις ιδιότητες :

1. Η det είναι γραμμική ως προς κάθε γραμμή.
2. Εάν δύο γραμμές ταυτίζονται τότε η det του πίνακα ισούται με μηδέν.
3. Η det οποιουδήποτε μεγέθους τετραγωνικού πίνακα, που έχει μονάδες στη κύρια διαγώνιο και μηδέν στις υπόλοιπες θέσεις, είναι μονάδα.

Το γεγονός ότι όντως υπάρχει μια τέτοια συνάρτηση και προσδιορίζεται μοναδικά από τις παραπάνω τρεις ιδιότητες αποδεικνύεται όπως ακριβώς και στο σώμα των μιγαδικών. Αυτή έχει όλες τις βασικές ιδιότητες που έχει κι εκεί. Ο ενδιαφερόμενος μπορεί να τις δει από το βιβλίο του Gilbert Strang που αναφέρεται στη βιβλιογραφία . Δύο από αυτές είναι ότι η det μπορεί να οριστεί με τις παραπάνω ιδιότητες αν αντί για γραμμές χρησιμοποιήσουμε στήλες, καθώς και ότι ένας τετραγωνικός πίνακας έχει γραμμικά ανεξάρτητες γραμμές και στήλες, δηλαδή είναι αντιστρέψιμος, αν και μόνο αν η det είναι διαφορετική του μηδέν (δηλαδή του ταυτοτικού στοιχείου της πρόσθεσης).

[35]Θεώρημα(Vandermonde)

Έστω $\rho_1,\ldots,\rho_n$ n στοιχεία ενός σώματος F και b φυσικός αριθμός, τότε η ορίζουσα det του $(n \times n)$ πίνακα

$$\begin{matrix} {\rho_1}^b & {\rho_1}^{b+1} & \ldots & {\rho_1}^{b+n-1} \\ {\rho_2}^b & {\rho_2}^{b+1} & \ldots & {\rho_2}^{b+n-1} \\ . & . & \ldots & . \\ . & . & \ldots & . \\ . & . & \ldots & . \\ {\rho_n}^b & {\rho_n}^{b+1} & \ldots & {\rho_n}^{b+n-1} \end{matrix}$$

δίνεται από τον τύπο $\prod_{i=1}^{n} {\rho_i}^b \cdot \prod_{i>j}(\rho_i - \rho_j)$ όπου το πρώτο σύμβολο εννοεί το γινόμενο όλων των ${\rho_i}^b$, από μία φορά, και το δεύτερο όλων των ($\binom{n}{2}$ πλήθους) δυνατών διαφορών, που ο πρώτος δείκτης είναι μεγαλύτερος του δεύτερου, από μία φορά.

Απόδειξη

Θα αποδείξουμε το Θεώρημα με επαγωγή. Υποθέτουμε ότι ισχύει τετριμμένα στη περίπτωση $n = 1,0$. Θεωρούμε τώρα δύο τυχαία στοιχεία ρ_1,ρ_2 του F και b τυχαίος φυσικός, τότε η ορίζουσα του πίνακα

$$\begin{matrix} {\rho_1}^b & {\rho_1}^{b+1} \\ {\rho_2}^b & {\rho_2}^{b+1} \end{matrix}$$

είναι ${\rho_1}^b{\rho_2}^{b+1} - {\rho_2}^b{\rho_2}^{b+1} = {\rho_1}^b{\rho_2}^b(\rho_2 - \rho_1)$ και ο τύπος επαληθεύτηκε.
Έστω τώρα ότι ο τύπος ισχύει για κάθε πίνακα αυτής της μορφής μέχρι μεγέθους $n - 1$. Θα το αποδείξουμε και για τον τυχαίο πίνακα της μορφής αυτής μεγέθους n

$$\begin{matrix} {\rho_1}^b & {\rho_1}^{b+1} & \ldots & {\rho_1}^{b+n-1} \\ {\rho_2}^b & {\rho_2}^{b+1} & \ldots & {\rho_2}^{b+n-1} \\ . & . & \ldots & . \\ . & . & \ldots & . \\ . & . & \ldots & . \\ {\rho_n}^b & {\rho_n}^{b+1} & \ldots & {\rho_n}^{b+n-1} \end{matrix}$$

Γνωρίζουμε ότι η ορίζουσα του πίνακα δεν αλλάζει εάν προσθέσουμε ένα πολλαπλάσιο μιας στήλης σε μία άλλη. Πηγαίνουμε τότε στη τελευταία στήλη $\Sigma(n)$ και της προσθέτουμε τη $-\rho_1\Sigma(n-1)$ κι ο πίνακας μετασχηματίζεται στον

$$\begin{matrix} {\rho_1}^b & {\rho_1}^{b+1} & \dots & 0 \\ {\rho_2}^b & {\rho_2}^{b+1} & \dots & {\rho_n}^{b+n-1} - \rho_1{\rho_2}^{b+n-2} \\ . & . & \dots & . \\ . & . & \dots & . \\ . & . & \dots & . \\ {\rho_n}^b & {\rho_n}^{b+1} & \dots & {\rho_n}^{b+n-1} - \rho_1{\rho_n}^{b+n-2} \end{matrix}$$

δηλαδή στον

$$\begin{matrix} {\rho_1}^b & {\rho_1}^{b+1} & \dots & 0 \\ {\rho_2}^b & {\rho_2}^{b+1} & \dots & (\rho_2-\rho_1){\rho_2}^{b+n-2} \\ . & . & \dots & . \\ . & . & \dots & . \\ . & . & \dots & . \\ {\rho_n}^b & {\rho_n}^{b+1} & \dots & (\rho_n-\rho_1)\,{\rho_n}^{b+n-2} \end{matrix}$$

Όμοια πηγαίνουμε στον νέο μας πίνακα και προσθέτουμε στη στήλη του $\Sigma(n-1)$ την $-\rho_1\Sigma(n-2)$ και κάνουμε το ίδιο. Συνεχίζουμε έτσι μέχρι να φτάσουμε στη δεύτερη στήλη $\Sigma(2)$ και να της προσθέσουμε την $-\rho_1\Sigma(1)$ και να προκύψει ο πίνακας

$$\begin{matrix} {\rho_1}^b & 0 & \dots & 0 \\ {\rho_2}^b & (\rho_2-\rho_1){\rho_2}^b & \dots & (\rho_2-\rho_1){\rho_2}^{b+n-2} \\ . & . & \dots & . \\ . & . & \dots & . \\ . & . & \dots & . \\ {\rho_n}^b & (\rho_n-\rho_1){\rho_n}^b & \dots & (\rho_n-\rho_1){\rho_n}^{b+n-2} \end{matrix}$$

Αυτός ο πίνακας έχει την ίδια ορίζουσα με τον αρχικό και γι αυτόν από γνωστές ιδιότητες της ορίζουσας ισχύει ότι η δικιά του ισούται με ${\rho_1}^b$ επί την ορίζουσα του πίνακα

$$\begin{matrix} (\rho_2-\rho_1){\rho_2}^b & \cdots & (\rho_2-\rho_1){\rho_2}^{b+n-2} \\ (\rho_3-\rho_1)\,{\rho_3}^b & \cdots & (\rho_3-\rho_1){\rho_3}^{b+n-2} \\ & \cdots & \cdot \\ \cdot & \cdots & \cdot \\ \cdot & \cdots & \cdot \\ (\rho_n-\rho_1){\rho_n}^b & \cdots & (\rho_n-\rho_1){\rho_n}^{b+n-2} \end{matrix}$$

του οποίου ισούται με $(\rho_2-\rho_1)(\rho_3-\rho_1)\ldots(\rho_n-\rho_1)$ επί την ορίζουσα του πίνακα

$$\begin{matrix} {\rho_2}^b & \cdots & {\rho_2}^{b+n-2} \\ {\rho_3}^b & \cdots & {\rho_3}^{b+n-2} \\ \cdot & \cdots & \cdot \\ \cdot & \cdots & \cdot \\ \cdot & \cdots & \cdot \\ {\rho_n}^b & \cdots & {\rho_n}^{b+n-2} \end{matrix}$$

ο οποίος είναι τετραγωνικός πίνακας βαθμού $n-1$ της επιθυμητής μορφής. Άρα γι αυτόν ισχύει η επαγωγική υπόθεση και η ορίζουσα του ισούται με $\prod_{i=1}^{n}{\rho_i}^b \cdot \prod_{i>j}(\rho_i-\rho_j)$, όπου το πρώτο σύμβολο εννοεί το γινόμενο όλων των ${\rho_i}^b$,από μία φορά, και το δεύτερο όλων των δυνατών διαφορών που ο πρώτος δείκτης είναι μεγαλύτερος του δεύτερου, από μία φορά. Από τα προηγούμενα αποτελέσματα συνδυαζόμενα όλα μαζί προκύπτει το ζητούμενο.

■

[36]<u>Θεώρημα</u>(Lagrange)

Έστω *H* μία υποομάδα μιας πεπερασμένης ομάδας *G*. Τότε η τάξη της *H* διαιρεί την τάξη της *G*.

<u>Απόδειξη</u>

Αν ορίσουμε μια σχέση ισοδυναμίας στο *G* όπου δύο στοιχεία του χ,*y* είναι ισοδύναμα εάν και μόνο αν το $\chi^{-1}y$ είναι στοιχείο της *H* το θεώρημα είναι προφανές. Το ότι αυτή η σχέση είναι όντως ισοδυναμία είναι τετριμμένο να αποδειχθεί.

■

[37]Λήμμα(Steinitz)

Έστω *V* διανυσματικός χώρος πάνω από το σώμα *K*, *X*=$\{\chi_1,\ldots,\chi_r\}$ ένα σύνολο του *V* από γραμμικώς ανεξάρτητα διανύσματα και *Y* = $\{y_1,\ldots,y_s\}$ ένα σύνολο γεννητόρων του V. Τότε ισχύουν

1. $r \leq s$
2. υπάρχει σύνολο γεννητόρων του *V* της μορφής $\{\chi_1,\chi_2,\ldots,\chi_r,y'_{r+1},\ldots,y'_s\}$ όπου y'_i στοιχεία του *Y*.

Απόδειξη

Αφού το *Y* είναι σύνολο γεννητόρων θα υπάρχει γραμμικώς συνδυασμός των στοιχείων του που μας δίνουν το χ_1. Διαλέγουμε ένα από αυτά και το αντικαθιστούμε με το χ_1. Το καινούριο μας σύνολο προφανώς παραμένει σύνολο γεννητόρων του *V* κι άρα θα υπάρχει γραμμικώς συνδυασμός των στοιχείων του που θα δίνει το χ_2 . Αυτό το άθροισμα θα πρέπει να περιέχει τουλάχιστον ένα στοιχείο διαφορετικό από το χ_1 αφού το *X* είναι γραμμικώς ανεξάρτητο. Διαλέγουμε ένα από αυτά και το αντικαθιστούμε με το χ_2, το καινούριο μας σύνολο προφανώς παραμένει γεννήτορας. Συνεχίζουμε έτσι μέχρι να προκύψει η 2 από την οποία έπεται και η 1.

■

Το Θεώρημα Kronecker είναι πολύ σημαντικό καθώς όχι μόνο μας αποδεικνύει ότι κάθε πολυώνυμο έχει ρίζα αλλά μας δίνει και μία μέθοδο να φτιάχνουμε επεκτάσεις σωμάτων που θα μας χρειαστούν για τη δημιουργία κωδίκων. Για κάθε δακτύλιο *R* ένας υποδακτύλιος του, *N*, για τον οποίο ισχύει ότι a*N* και *Nb* είναι υποσύνολα του *N* για κάθε a,*b* του *R*, ονομάζεται ιδεώδες του *R*. Μέγιστο ιδεώδες ενός δακτυλίου *R* λέμε ένα ιδεώδες *M* που είναι διαφορετικό από τον *R* και δεν περιέχεται γνήσια σε κανένα άλλο γνήσιο ιδεώδες *N* του *R*.

[38]Θεώρημα

Έστω *R* ένας αντιμεταθετικός δακτύλιος με μοναδιαίο στοιχείο. Τότε το *M* είναι μέγιστο ιδεώδες αν και μόνο αν ο *R*/*M* είναι σώμα.

Απόδειξη

Έστω *M* μέγιστο ιδεώδες του *R* και έστω πως ο *R*/*M* δεν είναι σώμα. Τότε θα υπάρχει στοιχείο a του *R* ώστε το a + *M* να μην έχει αντίστροφο. Θέτουμε *N* = {*r*a + *m* | για όλα τα *r* που ανήκουν στο *R* και *m* που ανήκουν στο *M*}. Το *N* προφανώς είναι ιδεώδες που περιέχει το *M*. Οπότε από τη μεγιστικότητα του *M* ισχύει *N* = *R*, επομένως υπάρχει *b* του *R* ώστε *b*a + *m* = 1, άρα το *b* + *M* είναι αντίστροφο του a + *M*, άτοπο. Αντίστροφα, έστω πως ο *R*/*M* είναι σώμα και ότι υπάρχει γνήσιο ιδεώδες *N* του *R* υπερσύνολο του *M*. Τότε το σύνολο με στοιχεία {*k* + *M* | για κάθε *k* ανήκει *N*} θα είναι προφανώς ιδεώδες του *R*/*M* μη τετριμμένο. Αυτό επεοδή αν *δ* ανήκει στο *N* αλλά όχι στο *M*, το *δ* + *M* είναι διαφορετικό του *M*. Τέλος θα είναι και γνήσιο αφού το 1 + M δεν ανήκει εκεί διότι αλλιώς θα

έπρεπε το 1 να ανήκει στο N που απαγορεύεται. Οπότε προκύπτει άτοπο γιατί ένα σώμα δεν έχει τέτοιου είδους ιδεώδη.

■

Αν F ένα σώμα και $F[\chi]$ η ακέραια περιοχή των πολυωνύμων του και $\gamma(\chi)$ ένα στοιχείο αυτής. Το σύνολο $\{ \alpha(\chi)\gamma(\chi) |$ για κάθε $\alpha(\chi)$ που ανήκει στο $F[\chi] \}$ συμβολίζεται $<\gamma(\chi)>$.

[39]Θεώρημα

Για κάθε ιδεώδες Γ του $F[\chi]$ ενός σώματος F, υπάρχει στοιχείο του $\lambda(\chi)$, ώστε, $<\lambda(\chi)> = \Gamma$.

Απόδειξη

Έστω $\lambda(\chi)$ ένα στοιχείο του Γ που έχει το μικρότερο βαθμό από αυτά. Τότε αν $\gamma(\chi)$ ανήκει στο Γ από τον αλγόριθμό της διαίρεσης θα υπάρχουν πολυώνυμα $\pi(\chi),\upsilon(\chi)$ του $F[\chi]$ ώστε $\gamma(\chi) = \pi(\chi)\lambda(\chi) + \upsilon(\chi)$, όπου το $\upsilon(\chi)$ θα έχει βαθμό μικρότερο του $\lambda(\chi)$. Άρα αφού Γ ιδεώδες $\upsilon(\chi) = 0$.

■

[40]Θεώρημα

Ένα ιδεώδες $<p(\chi)>$ στον $F[\chi]$ είναι μέγιστο, αν και μόνο αν, το $p(\chi)$ είναι ανάγωγο.

Απόδειξη

Αν το $p(\chi)$ είναι ανάγωγο και το $<p(\chi)>$ δεν ήταν μέγιστο, τότε θα υπήρχε $\lambda(\chi)$ στοιχείο του $F(\chi)$ ώστε το $<\lambda(\chi)>$ να είναι διαφορετικό του $F[\chi]$ και να περιέχει το $<p(\chi)>$ ως γνήσιο υποσύνολο. Τότε θα υπάρχει $k(\chi)$ του $F(\chi)$ ώστε $p(\chi) = k(\chi)\lambda(\chi)$, άτοπο αν $k(\chi)$ δεν είναι σταθερό πολυώνυμο, όμως και σε αυτή την περίπτωση έχουμε άτοπο αφού έτσι προκύπτει $<p(\chi)> = <\lambda(\chi)>$. Αντίστροφα, το $<p(\chi)>$ ήταν μέγιστο χωρίς το $p(\chi)$ να είναι ανάγωγο, θα υπήρχαν πολυώνυμα $k(\chi),\lambda(\chi)$ όχι σταθερά, του $F[\chi]$ ώστε $p(\chi) = k(\chi)\lambda(\chi)$. Άρα το $<k(\chi)>$ θα ήταν ένα γνήσιο μη τετριμμένο ιδεώδες που περιέχει ως υποσύνολο το $<p(\chi)>$, άτοπο.

■

[41]Θεώρημα (Kronecker)

Έστω F ένα σώμα και $f(\chi)$ ένα μη σταθερό πολυώνυμο στον $F[\chi]$. Τότε υπάρχει μία επέκταση σώματος E του F ώστε να υπάρχει a που ανήκει στην E και $f(a) = 0$.

Απόδειξη

Αν το $f(\chi)$ έχει ρίζα στο F το θεώρημα ισχύει τετριμμένα. Έστω ότι δεν έχει, τότε αν το $f(\chi)$ δεν είναι ανάγωγο πάνω από το F μπορούμε με επαγωγή να βρούμε ένα πολυώνυμο $p(\chi)$ του $F[\chi]$ που διαιρεί το $f(\chi)$ και να είναι. Αν βρούμε μία επέκταση που περιέχει μία ρίζα του p(χ) έχουμε τελειώσει. Από τα Θεωρήματα[39],[37] το $F[\chi]/<p(\chi)>$ είναι σώμα. Θεωρούμε τον ομομορφισμό ψ:F → $F[\chi]/<p(\chi)>$ που ορίζεται από τις σχέσεις $\psi(a) = a + <p(\chi)>$ για κάθε a του F και $\psi(\chi) = \chi + <p(\chi)>$. Η ψ είναι 1-1 αφού αν $a + <p(\chi)> = b + <p(\chi)>$ τότε $(a - b) + <p(\chi)> = <p(\chi)>$ κι άρα $a - b$ στοιχείο του $<p(\chi)>$, άτοπο. Οπότε είναι φανερό πως πρόκειται για ισομορφισμό. Θα δείξουμε ότι το $E = F[\chi]/<p(\chi)>$ είναι το σώμα που ζητάμε . Σε αυτό μπορούμε να κοιτάμε κάθε στοιχείο ψ(a) σαν να ήταν το a. Έτσι αν $p(\chi) = p_0 + \ldots + p_n\chi^n$ το μεταφέρουμε στο E ως το $(p_0 + <p(\chi)>) + \ldots + (p_n + <p(\chi)>)\chi^n$ κι βλέπουμε αμέσως ότι το
$\chi + <p(\chi)>$ είναι ρίζα του. Άρα αν πάμε στο E κι αλλάξουμε τον συμβολισμό των στοιχείων $a + <p(\chi)>$ σε a, όπου a ανήκει στο F έχουμε τελειώσει.

■

[42]Θεώρημα(Frobenius)

Έστω F ένα πεπερασμένο σώμα χαρακτηριστικής p. Τότε η απεικόνιση σ_p:F→F που ορίζεται από τη σχέση $\sigma_p(a) = a^p$,για κάθε a του F, είναι αυτομορφισμός και λέγεται αυτομορφισμός του Frobenius.

Απόδειξη

Από τον διωνυμικό τύπο έχουμε $(a + b)^p = \sum_{k=0}^{p} \binom{p}{k} a^k b^{p-k}$
οπότε λόγο ότι p είναι η χαρακτηριστική του σώματος και p πρώτος, θα έχουμε ότι $(a + b)^p = a^p + b^p$. Προφανώς $(ab)^p = a^p b^p$, άρα η σ_p είναι 1-1 και ομομορφισμός. Αυτό σε συνδυασμό με το ότι το F είναι πεπερασμένο σώμα ολοκληρώνει την απόδειξη.

■

Προφανώς και η αντίστροφή της θα είναι αυτομορφισμός όπως και οποιεσδήποτε δυνάμεις τους.

Χρησιμοποιώντας τον αυτομορφισμό του Frobenius μπορούμε να δείξουμε το ακόλουθο: Έστω ένα σώμα F χαρακτηριστικής p και μεγέθους p^s, μια επέκταση του K μεγέθους $(p^s)^r$ και ένα πολυώνυμο $f(\chi)$ με συντελεστές στο F. Για κάθε a που ανήκει στο K, αυτό είναι ρίζα του $f(\chi)$, αν και μόνο αν, το a^{p^s} είναι ρίζα του $f(\chi)$. Αυτό ισχύει διότι η σ_p σύμφωνα με τη παραπάνω απόδειξη είναι αυτομορφισμός στο K όπως και η ${\sigma_p}^{-1}$. Οπότε οι ${\sigma_p}^s$, $({\sigma_p}^{-1})^s$ θα είναι και αυτές αυτομορφισμοί στο K. Λόγο του Θεωρήματος Lagrange για τα στοιχεία του F ισχύει πως αυτά είναι ρίζες του πολυωνύμου $\chi^{p^s} - \chi$. Επομένως το F παραμένει σταθερό πάνω από τους αυτομορφισμούς ${\sigma_p}^s$, $({\sigma_p}^{-1})^s$ κι άρα έχουμε πως $0 = {\sigma_p}^s(f(a)) = f({\sigma_p}^s(a)) = f(a^{p^s})$ και αντίστροφα $0 = ({\sigma_p}^{-1})^s(f(a^{p^s})) = f(({\sigma_p}^{-1})^s(a^{p^s})) = f(a)$.

Κεφάλαιο 3

Κώδικες Reed - Solomon

3.1 Συμβατικοί Reed – Solomon

Στο κεφάλαιο αυτό γίνεται η μελέτη των κωδίκων Reed-Solomon. Είναι μια κατηγορία με πολλές καλές ιδιότητες για τη δημιουργία της οποίας θα χρειαστούν όλα τα προηγούμενα αποτελέσματα που αναφέρθηκαν. Ξεκινάμε με τους συμβατικούς κώδικες Reed-Solomon.

Έστω F ένα σώμα με q στοιχεία, από όσα έχουμε πει το q θα είναι δύναμη κάποιου πρώτου. Θα θέλαμε με βάση αυτό το τυχαίο σώμα F να φτιάξουμε ένα κώδικα μήκους n, όπου n τυχαίος φυσικός αριθμός, δηλαδή μπορεί και μεγαλύτερος ή ίσος του q. Υπάρχουν άπειροι φυσικοί έτσι ώστε αν υψώσεις το q σε αυτούς θα δώσουν αριθμό μεγαλύτερο του n. Διαλέγουμε έναν από αυτούς έστω s. Από το Πόρισμα[33] του Κεφαλαίου 2 υπάρχει ένα ανάγωγο πολυώνυμο βαθμού s στον $F[\chi]$, γι αυτό θα υπάρχει, φ, στοιχείο της αλγεβρικής θήκης του F το οποίο θα είναι ρίζα του. Άρα η αλγεβρική επέκταση $K = F(\varphi)$ του F θα έχει $q^s \geq n + 1$ στοιχεία. Από το Θεώρημα[28] του Κεφαλαίου 2 η ομάδα των μη μηδενικών στοιχείων του σώματος K με πράξη το πολλαπλασιασμό θα είναι κυκλική. Έστω a ένας γεννήτορας αυτής, ορίζουμε το πολυώνυμο $\gamma(\chi)$ του $K[\chi]$ ως εξής : έστω b τυχαίος φυσικός αριθμός και δ φυσικός για τον οποίο ισχύει
$2 \leq \delta \leq n$, τότε

$$\gamma(\chi) = (\chi - a^b) \cdot (\chi - a^{b+1}) \cdot \ldots \cdot (\chi - a^{b+\delta-2}).$$

Λόγο του περιορισμού του δ τα στοιχεία $a^b, a^{b+1}, \ldots, a^{b+\delta-2}$ είναι διαφορετικά ανά δύο.

[1]Ορισμός

Ο πολυωνυμικός κώδικας $CRS = CRS[n,\delta,a,b]$ μήκους n, με πολυώνυμο γεννήτορα το $\gamma(\chi)$ του $K[\chi]$, ονομάζεται, *συμβατικός κώδικας Reed-Solomon* προσχεδιασμένης απόστασης δ (με σώμα βάσης το F).

Είναι προφανές από όσα έχουν προηγηθεί για τους πολυωνυμικούς κώδικες ότι ο $CRS[n,\delta,a,b]$ θα μπορούσε να ορισθεί και σαν τα στοιχεία του K^n που είναι τα διανύσματα με τις συντεταγμένες τους να είναι οι συντελεστές των πολυωνύμων του $K_{n-1}[\chi]$ που έχουν ως ρίζες όλα τα στοιχεία $a^b, \ldots, a^{b+\delta-2}$.

Πρωταρχικοί συμβατικοί κώδικες CRS ονομάζονται αυτοί που έχουν μήκος $n = |K| - 1$. Δηλαδή το μήκος τους ισούται όσο το πλήθος της πολλαπλασιαστικής ομάδας των μη μηδενικών στοιχείων του K. Άρα επειδή από το Θ.Lagrange κάθε στοιχείο του K είναι ρίζα

του $\chi^{|K|-1}-1$, αν $(a_0,a_1,\ldots a_{n-1})$ ένα διάνυσμα του κώδικα, για τους λόγους που είπαμε το πολυώνυμο $a_0+a_1\chi+\ldots+a_{n-1}\chi^{n-1}$ θα έχει ρίζα του όλα τα $a^b,\ldots,a^{b+\delta-2}$, όπως και το $(a_0+a_1\chi+\ldots+a_{n-1}\chi^{n-1})\cdot\chi$. Στο τελευταίο πολυώνυμο οι τιμές που δίνει όταν αντικατασταθεί το χ με οποιοδήποτε μη μηδενικό στοιχείο του K, επειδή $a_{n-1}\chi^n = a_{n-1}$ για κάθε χ στο K, ταυτίζονται με αυτές του $a_{n-1}+a_0\chi+\ldots+a_{n-2}\chi^{n-1}$. Άρα κι αυτό θα έχει όλα τα $a^b,\ldots,a^{b+\delta-2}$ ως ρίζες. Έτσι το διάνυσμα $(a_{n-1},a_0,\ldots,a_{n-2})$ ανήκει κι αυτό στον κώδικα, επομένως στην περίπτωση που $n = |K|-1$ εκεί ο κώδικας είναι και κυκλικός.

Είναι εύκολο να δει κάποιος ότι ο πίνακας

$$H=\begin{matrix}1 & a^b & (a^b)^2 & \ldots & (a^b)^{n-1}\\ 1 & a^{b+1} & (a^{b+1})^2 & \ldots & (a^{b+1})^{n-1}\\ . & . & . & \ldots & .\\ . & . & . & \ldots & .\\ . & . & . & \ldots & .\\ 1 & a^{b+\delta-2} & (a^{b+\delta-2})^2 & \ldots & (a^{b+\delta-2})^{n-1}\end{matrix}$$

είναι ένας πίνακας ελέγχου ισοτιμίας για τον *CRS*[*n*,*δ*,a,*b*], αφού για ένα διάνυσμα του K^n, $c=(c_0,c_1,\ldots,c_{n-1})$, ισχύει, $0 = c\cdot H^* = H\cdot c^*$,αν και μόνο αν, τα στοιχεία του *c* είναι συντελεστές πολυωνύμου του $K[\chi]$ που έχει ρίζες τα $a^b,\ldots,a^{b+\delta-2}$.

[2]Θεώρημα

Ένας κώδικας Reed-Solomon *CRS*(*n*,*δ*,a,*b*) με πολυώνυμο γεννήτορα $\gamma(\chi)$ είναι κώδικας MDS. Μάλιστα για την ελάχιστη απόσταση του *d* ισχύει $\deg(\gamma(\chi))+1 = d = \delta$.

Απόδειξη

Από την Πρόταση [29] και τα σχόλια μετά τον Ορισμό [30] του Κεφαλαίου 1 προκύπτει ότι η διάσταση του κώδικα CRS[*n*,*δ*,a,*b*] θα είναι $n-(\delta-1)$. Ακόμα από ότι είδαμε ο *H* είναι πίνακας ισοτιμίας για τον κώδικα, αν τον δούμε αυτόν ως τη γραμμική συνάρτηση $y = H\cdot c^*$ από τον K^n στον $K^{\delta-1}$ θα πρέπει η διάσταση της εικόνας $y(K^n)$, η οποία ισούται με τη τάξη του πίνακα, να είναι $n-\dim\ker f$,όμως η διάσταση του πυρήνα είναι όσο του κώδικα, άρα $\dim\ker f = n-(\delta-1)$. Δηλαδή η τάξη του πίνακα θα είναι ίση με $\delta-1$. Γνωρίζουμε από τον περιορισμό για το *δ* ότι, $\delta-1\le n-1$, άρα αφού ο πίνακας *H* έχει *n* στήλες θα υπάρχει ένα υποσύνολο αυτών με πλήθος *δ* οι οποίες θα είναι γραμμικώς εξαρτημένες. Οπότε από τη Πρόταση[25] του Κεφαλαίου 1 θα ισχύει για την ελάχιστη απόσταση του *CRS*[*n*,*δ*,a,*b*] , *d*, ότι

$d \leq \delta$. Θα δείξουμε με άτοπο ότι δεν γίνεται να υπάρχει υποσύνολο των στηλών οι οποίες θα είναι γραμμικώς εξαρτημένες με πλήθος μικρότερο από δ. Έστω ότι υπήρχε ένα τέτοιο σύνολο, τότε, εάν χρειαστεί το συμπληρώνουμε με κατάλληλο αριθμό τυχαία επιλεγμένων στηλών από τις περισευούμενες για να γίνει πλήθους $\delta - 1$ και σχηματίζουμε των $(\delta - 1) \times (\delta - 1)$ πίνακα τους ώστε οι δυνάμεις να μπαίνουν σε αύξουσα σειρά. Δηλαδή φτιάχνουμε τον πίνακα Γ, όπου

$$\Gamma = \begin{matrix} (a^b)^{l_1} & (a^b)^{l_2} & \dots & (a^b)^{l_{\delta-1}} \\ (a^{b+1})^{l_1} & (a^{b+1})^{l_2} & \dots & (a^{b+1})^{l_{\delta-1}} \\ . & . & \dots & . \\ . & . & \dots & . \\ . & . & \dots & . \\ (a^{b+\delta-2})^{l_1} & (a^{b+\delta-2})^{l_2} & \dots & (a^{b+\delta-2})^{l_{\delta-1}} \end{matrix}$$

όπου $l_1 \leq l_2 \leq \ldots \leq l_{\delta-1}$ οι εκθέτες του συνόλου των στηλών. Η τάξη του Γ θα είναι η ίδια με του ανάστροφου του, Γ^*

$$\Gamma^* = \begin{matrix} (a^b)^{l_1} & (a^{b+1})^{l_1} & \dots & (a^{b+\delta-2})^{l_1} \\ (a^b)^{l_2} & (a^{b+1})^{l_2} & \dots & (a^{b+\delta-2})^{l_2} \\ . & . & \dots & . \\ . & . & \dots & . \\ . & . & \dots & . \\ (a^b)^{l_{\delta-1}} & (a^{b+1})^{l_{\delta-1}} & \dots & (a^{b+\delta-2})^{l_{\delta-1}} \end{matrix}$$

ο οποίος γράφεται και ως

$$\Gamma^* = \begin{matrix} (a^{l_1})^b & (a^{l_1})^{b+1} & \dots & (a^{l_1})^{b+\delta-2} \\ (a^{l_2})^b & (a^{l_2})^{b+1} & \dots & (a^{l_2})^{b+\delta-2} \\ . & . & \dots & . \\ . & . & \dots & . \\ . & . & \dots & . \\ (a^{l_{\delta-1}})^b & (a^{l_{\delta-1}})^{b+1} & \dots & (a^{l_{\delta-1}})^{b+\delta-2} \end{matrix}$$

που είναι πίνακας της μορφής για της οποίας μιλήσαμε στο τέλος του κεφαλαίου2. Άρα σύμφωνα με το Θεώρημα Vandermonde, για την ορίζουσα του det, θα ισχύει,
$\det(\Gamma^*) = \prod_{i=1}^{\delta-1} (a^{l_i})^b \cdot \prod_{i>j} (a^{l_i} - a^{l_j})$ όπου το πρώτο σύμβολο εννοεί το γινόμενο όλων των $(a^{l_i})^b$, από μία φορά, και το δεύτερο όλων των δυνατών διαφορών που ο πρώτος δείκτης είναι μεγαλύτερος του δεύτερου, από μία φορά. Όπως έχουμε αναφέρει λόγο των ρυθμίσεων στις παραμέτρους του κώδικα *CRS* τα a^{l_i} είναι διακεκριμένα, άρα οι όροι και στα δύο γινόμενα είναι διάφοροι του μηδενός, οπότε και η ορίζουσα θα είναι μη μηδενική αφού το K είναι σώμα.

Επομένως από τις παρατηρήσεις πριν από το Θεώρημα[35] του Κεφαλαίου 2 οι στήλες του Γ είναι γραμμικώς ανεξάρτητες, άτοπο.
Από τα παραπάνω προκύπτει ότι deg($\gamma(\chi)$) + 1 = δ = *d*. Από την Πρόταση[15] του Κεφαλαίου 1, για γραμμικούς κώδικες ισχύει d ≤ n – k + 1, όπου *k* η διάσταση του κώδικα. Στη περίπτωση μας $k = n - (\delta - 1)$ άρα η προηγούμενη ανισότητα γίνεται $d \leq \delta$ και το Θεώρημα αποδείχθηκε.
■

3.2 *BCH*

Πριν περάσουμε στο τελικό στάδιο που είναι οι γενικευμένοι κώδικες Reed-Solomon θα παρουσιάσουμε τους κώδικες *BCH*. Αυτοί ορίζονται ως εξής:

Έστω *F* ένα πεπερασμένο σώμα με *q* στοιχεία και *n*,*δ* φυσικοί με $2 \leq \delta \leq n$. Έστω *K* μία επέκταση του *F*, βαθμού *s*, με την ιδιότητα $q^s \geq n + 1$ και a ένα στοιχείο γεννήτορας των μη μηδενικών στοιχείων του *K*. Κατασκευάζουμε των κώδικα *CRS*(*n*,*δ*,a,*b*) και παίρνουμε την τομή του με των διανυσματικό χώρο F^n , έστω *A*, δηλαδή $A = CRS[n,\delta,a,b] \cap F^n$. Προφανώς αφού οι *CRS*[*n*,*δ*,a,*b*], F^n είναι υπόχωροι του K^n και το *A* θα είναι υπόχωρος του K^n και πιο συγκεκριμένα του F^n. Το σύνολο *A* είναι ένας γραμμικώς υποκώδικας του *CRS*[*n*,*δ*,a,*b*] κι άρα η ελάχιστη απόσταση του θα είναι τουλάχιστον *δ*.

Δηλαδή τα στοιχεία του *A* είναι τα διανύσματα οι συντεταγμένες των οποίων είναι οι συντελεστές των πολυωνύμων του $F_{n-1}[\chi]$ που ανάμεσα στις ρίζες τους βρίσκονται όλα τα στοιχεία $a^b,\ldots,a^{b+\delta-2}$. Το σύνολο *A* είναι ο κώδικας *BCH* = *BCH*[*n*,*δ*,a,*b*] και είναι προφανώς μη κενό αφού η επέκταση *K* του *F* ως πεπερασμένη είναι και αλγεβρική.

3.3 Γενικευμένοι Reed – Solomon

Το τελευταίο στάδιο είναι οι *γενικευμένοι κώδικες Reed-Solomon,* συμβολισμός *GRS*. Ξεκινάμε από ένα πεπερασμένο σώμα *F* μεγέθους *q* και παίρνουμε από αυτό $a_1,\ldots,a_n$ μη μηδενικά διακεκριμένα στοιχεία και $u_1,u_2,\ldots,u_n$ πάλι μη μηδενικά χωρίς όμως τον περιορισμό αυτά να μην επαναλαμβάνονται. Ακόμα έστω *δ* ένας φυσικός όπου $2 \leq \delta \leq n$. Τότε ο *GRS* κώδικας μας είναι ο γραμμικός κώδικας με πίνακα ελέγχου ισοτιμίας $H = \Sigma \cdot U$ όπου

$$\Sigma = \begin{matrix} 1 & 1 & . & \ldots & 1 \\ a_1 & a_2 & . & \ldots & a_n \\ a_1^{\,2} & a_2^{\,2} & . & \ldots & a_n^{\,2} \\ . & . & . & \ldots & \\ . & . & . & \ldots & . \\ . & . & . & \ldots & . \\ a_1^{\,\delta-2} & a_2^{\,\delta-2} & . & \ldots & a_n^{\,\delta-2} \end{matrix}$$

και

$$U = \begin{matrix} u_1 & 0 & 0 & \dots & 0 \\ 0 & u_2 & 0 & \dots & 0 \\ 0 & 0 & u_3 & \dots & 0 \\ . & . & . & \dots & . \\ . & . & . & \dots & . \\ . & . & . & \dots & . \\ 0 & 0 & 0 & \dots & u_n \end{matrix}$$

Όπως βλέπουμε το μήκος του κώδικα *GRS* είναι *n* για το οποίο ισχύει, $n \leq q - 1$. Τα στοιχεία u_i ονομάζονται συντελεστές στηλών ενώ τα στοιχεία a_i εντοπισμοί του πίνακα. Το νόημα πίσω από αυτές τις ονομασίες θα δοθεί παρακάτω.

Αν a ένα πρωταρχικό στοιχείο του σώματος *F* και *b* ένας μη αρνητικός ακέραιος, θέτοντας $a_i = a^{i-1}$ και $u_i = a^{b(i-1)}$ παρατηρούμε ότι ο πίνακας ισοτιμίας ταυτίζεται με αυτόν ενός συμβατικού κώδικα *CRS*[*n*,*δ*,a,*b*].

Θέτουμε $k = n - (\delta - 1)$. Το *k* παίζει το ρόλο της διάστασης του κώδικα. Αυτό διότι γνωρίζουμε ότι αυτή θα πρέπει να ισούται με το *n* μείον τη τάξη του *H*. Στη περίπτωση μας η τάξη του *H* ταυτίζεται με την τάξη του *Σ*, αφού ο *U* λόγο της δομής του δεν επηρεάζει κάπου. Ο *Σ* τώρα έχει $(\delta - 1)$ γραμμικώς ανεξάρτητες γραμμές, επομένως ισχύει το ζητούμενο.

Η αιτιολόγηση είναι σωστή διότι αν οι γραμμές του *Σ* ήταν γραμμικώς εξαρτημένες, τότε θα υπήρχε διάνυσμα c μη μηδενικό του $F^{\delta-1}$ ώστε $c \cdot \Sigma = 0$. Αυτό όμως σημαίνει ότι το πολυώνυμο με συντελεστές τα στοιχεία του *c* βαθμού το πολύ $(\delta - 2)$ έχει *n* διακεκριμένες ρίζες, άτοπο αφού $(\delta - 2) \leq n - 2$.

[3]<u>Θεώρημα</u>
Ένας γενικευμένος κώδικας Reed-Solomon *GRS* είναι ένας κώδικας με παραμέτρους [*n*, *k*, $d = n - k + 1$], δηλαδή ένας μέγιστης ελάχιστης απόστασης (MDS).

<u>Απόδειξη</u>

Λόγο της δομής του *H* για να αποδείξουμε ότι το $d = n - k + 1$ με τη βοήθεια της Πρότασης[25] του Κεφαλαίου 1, αρκεί να μελετήσουμε τον πίνακα *Σ* σαν να ήταν ο πίνακας ισοτιμίας. Όπως
αναφέραμε στα σχόλια παραπάνω ο *Σ* έχει τάξη όσες και οι γραμμές του, δηλαδή $\delta - 1$, άρα ισχύει $d \leq \delta$. Θέλουμε να δείξουμε ότι ο *Σ* δεν μπορεί να έχει ένα σύνολο από *λ*, με $\lambda \leq \delta - 1$ γραμμικώς εξαρτημένες στήλες. Έστω ότι είχε, τις συμπληρώνουμε με κατάλληλο αριθμό τυχαία επιλεγμένων στηλών από τις περισευούμενες για να γίνουν $\delta - 1$ στο πλήθος και έστω ότι αυτές είναι οι Σ_{λ_1}, ..., $\Sigma_{\lambda_{\delta-1}}$. Τις γράφουμε τη μία δίπλα στην άλλη και φτιάχνουμε ένα καινούριο $(\delta - 1) \times (\delta - 1)$ πίνακα με στήλες γραμμικώς εξαρτημένες. Ο ανάστροφος αυτού του πίνακα είναι μορφής Vandermonde, άρα, επειδή $a_1, \dots, a_n$ διακεκριμένα μη μηδενικά, ο τελευταίος θα έχει μη μηδενική ορίζουσα, άτοπο.

■

Αν ο γενικευμένος κώδικας μας έχει μήκος $n = q - 1$, ονομάζεται *πρωταρχικός*.

Εάν οι συντελεστές στηλών είναι ίσοι με τα αντίστοιχα στοιχεία εντοπισμού, $a_i = u_i$, τότε ο κώδικας λέγεται, *υπό την στενή έννοια γενικευμένος κώδικας Reed-Solomon*.

Στην περίπτωση που όλοι οι συντελεστές στηλών είναι ίσοι με τη μονάδα ο κώδικας θα ονομάζεται *κανονικοποιημένος*.

Τώρα θα δείξουμε ότι ο δυικός ενός γενικευμένου κώδικα Reed-Solomon είναι κι αυτός γενικευμένος κώδικας Reed-Solomon. Έστω F ένα πεπερασμένο σώμα με q το πλήθος στοιχεία και C ένας *GRS* γενικευμένος κώδικας Reed-Solomon με παραμέτρους $[n,k,n-k+1]$ και πίνακα ελέγχου ισοτιμίας $H = \Sigma \cdot U$, όπου

$$\Sigma = \begin{matrix} 1 & 1 & . & \dots & 1 \\ a_1 & a_2 & . & \dots & a_n \\ a_1^{\,2} & a_2^{\,2} & . & \dots & a_n^{\,2} \\ . & . & . & \dots & . \\ . & . & . & \dots & . \\ . & . & . & \dots & . \\ a_1^{\,\delta-2} & a_2^{\,\delta-2} & . & \dots & a_n^{\,\delta-2} \end{matrix}$$

και

$$U = \begin{matrix} u_1 & 0 & 0 & \dots & 0 \\ 0 & u_2 & 0 & \dots & 0 \\ 0 & 0 & u_3 & \dots & 0 \\ . & . & . & \dots & . \\ . & . & . & \dots & . \\ . & . & . & \dots & . \\ 0 & 0 & 0 & \dots & u_n \end{matrix}$$

όπου $(\delta - 2) = n - k - 1$. Από το Θεώρημα[27] του Κεφαλαίου 1 και ο $C^{\perp}$ θα είναι MDS κώδικας με παραμέτρους $[n,n-k,k+1]$. Ψάχνουμε τώρα για τον $C^{\perp}$ ένα πίνακα ελέγχου ο οποίος θα είναι στην μορφή που έχουν οι πίνακες *GRS*. Κατασκευάζουμε τον $J = B \cdot V$ όπου

$$B = \begin{matrix} 1 & 1 & \dots & 1 \\ a_1 & a_2 & \dots & a_n \\ . & . & \dots & . \\ . & . & \dots & . \\ . & . & \dots & . \\ a_1^{\,k-1} & a_2^{\,k-1} & \dots & a_n^{\,k-1} \end{matrix}$$

και

$$V = \begin{matrix} v_1 & 0 & \dots & 0 \\ 0 & v_2 & \dots & 0 \\ . & . & \dots & . \\ . & . & \dots & . \\ . & . & \dots & . \\ 0 & 0 & \dots & v_n \end{matrix}$$

όπου τα v_i είναι όλα διαφορετικά του μηδενός.
Αν δείξουμε ότι υπάρχει κατάλληλος πίνακας V ώστε $J \cdot H^* = 0$ έχουμε τελειώσει, διότι από την Πρόταση[23] του Κεφαλαίου ο 1, ο J θα είναι γεννήτορας πίνακας του C και πίνακας ισοτιμίας για τον $C^{\perp}$, αφού ο B έχει τάξη $k = n - (n - k)$. Ο B έχει τάξη k επειδή οι γραμμές του είναι γραμμικώς ανεξάρτητες. Αυτό συμβαίνει γιατί αν δεν ήταν θα υπήρχε διάνυσμα του F^k του οποίου τα στοιχεία θα ήταν οι συντελεστές ενός πολυωνύμου του $F_{k-1}[\chi]$ ώστε αυτό το πολυώνυμο να είχε τα $a_1,\dots,a_n$ ρίζες, όμως τότε ένα πολυώνυμο βαθμού το πολύ $k - 1$ θα έχει n διακεκριμένες ρίζες, άτοπο.
Εκτελόντας τις πράξεις στην ισότητα $J \cdot H^* = 0$, καταλήγουμε στη σχέση $\Lambda^* \cdot \Sigma^* = 0$, όπου

$$\Lambda = \begin{matrix} u_1v_1 & u_1v_1a_1 & \dots & u_1v_1{a_1}^{k-1} \\ u_2v_2 & u_2v_2\,a_2 & \dots & u_2v_2{a_2}^{k-1} \\ . & . & \dots & . \\ . & . & \dots & . \\ . & . & \dots & . \\ u_nv_n & u_nv_na_n & \dots & u_nv_n{a_n}^{k-1} \end{matrix}$$

Άρα αν θέσω $\Gamma = \Lambda^* \cdot \Sigma^*$ θα πρέπει $\Gamma = 0$, όπου Γ είναι ο $(k \times (n - k))$ πίνακας του οποίου σε κάθε θεση (i,j) $0 \le i \le k - 1$, $0 \le j \le n - k - 1$, το στοιχείο του χ(i,j) είναι το χ(i,j) = $\sum_{r=1}^{n}(u_r v_r {a_r}^{(i+j)})$. Αυτό είναι ισοδύναμο με το σύστημα $T \cdot v = 0$ όπου

$$T = \begin{matrix} u_1 & u_2 & \dots & u_n \\ u_1a_1 & u_2a_2 & \dots & u_na_n \\ . & . & \dots & . \\ . & . & \dots & . \\ . & . & \dots & . \\ u_1{a_1}^{n-2} & u_2{a_2}^{n-2} & \dots & u_n{a_n}^{n-2} \end{matrix} \quad \text{και} \quad v = \begin{matrix} v_1 \\ v_2 \\ . \\ . \\ . \\ v_n \end{matrix}$$

Ο πίνακας T είναι ένας πίνακας με τάξη $n - 1$ διότι ισχύει πως $T = T' \cdot U$, όπου

$$T' = \begin{matrix} 1 & 1 & \dots & 1 \\ a_1 & a_2 & \dots & a_n \\ . & . & \dots & . \\ . & . & \dots & . \\ . & . & \dots & . \\ a_1^{n-2} & a_2^{n-2} & \dots & a_n^{n-2} \end{matrix}$$

και άρα ο *T* έχει *n* – 1 γραμμικώς ανεξάρτητες γραμμές. Αυτό γιατί, όπως έχουμε αναφέρει πολλές φορές, αν δεν ήταν θα υπήρχε διάνυσμα του F^{n-1} του οποίου τα στοιχεία θα ήταν οι συντελεστές ενός πολυωνύμου του $F_{n-1}[\chi]$ ώστε αυτό το πολυώνυμο να είχε τα $a_1,\dots,a_n$ ρίζες. Όμως τότε ένα πολυώνυμο βαθμού το πολύ *n* – 1 θα είναι n διακεκριμένες ρίζες, άτοπο. Δηλαδή ο χώρος των λύσεων θα είναι μονοδιάστατος. Έστω το μη μηδενικό στοιχείο, *v*, ανήκει σε αυτόν. Τότε θα πρέπει όλες οι συντεταγμένες του *v* να είναι μη μηδενικές, διότι όπως αναφέραμε $T = T' \cdot U$, άρα ο πίνακας αυτός είναι ένας πίνακας ελέγχου ισοτιμίας για ένα *GRS* κώδικα με παραμέτρους [*n*,1,*n*]. Οπότε αν το *v* ικανοποιεί την σχέση $T \cdot v = 0$ θα πρέπει να είναι στοιχείο αυτού του *GRS* κι άρα να έχει βάρος *n*. Οπότε δείξαμε το

[4]Θεώρημα

Έστω *C* ένας *GRS* [*n*, *k*, *n* – *k* + 1] γενικευμένος κώδικας Reed-Solomon επί ενός πεπερασμένου σώματος *F*. Τότε ο δυικός του κώδικας $C^{\perp}$ είναι επίσης ένας [*n*, *n* – *k*, *k* + 1] γενικευμένος κώδικας Reed-Solomon. Μάλιστα και οι δύο μπορούν να οριστούν επί των ίδιων εντοπισμών $a_1,\dots,a_n$.

Απόδειξη

Προηγηθηκε. ∎

Από το Θεώρημα [4] και από όσα είπαμε στο Κεφάλαιο 1 ένας κώδικας Reed-Solomon έχει ένα γεννήτορα πίνακα της μορφής $B \cdot V$ όπου

$$B = \begin{matrix} 1 & 1 & \dots & 1 \\ a_1 & a_2 & \dots & a_n \\ . & . & \dots & . \\ . & . & \dots & . \\ . & . & \dots & . \\ a_1^{k-1} & a_2^{k-1} & \dots & a_n^{k-1} \end{matrix}$$

και

$$V = \begin{matrix} v_1 & 0 & \dots & 0 \\ 0 & v_2 & \dots & 0 \\ . & . & \dots & . \\ . & . & \dots & . \\ . & . & \dots & . \\ 0 & 0 & \dots & v_n \end{matrix}$$

όπου τα v_i είναι όλα διαφορετικά του μηδενός.
Φυσικά, ταυτόχρονα, ο $B \cdot V$ είναι ένας πίνακας ελέγχου ισοτιμίας του δυικού του.
Άρα αν ταυτίσουμε την προς κωδικοποίηση λέξη $c = (c_0,\dots,c_{k-1})$ με το πολυώνυμο $\varphi(\chi) = c_0 + \dots + c_{k-1}\chi^{k-1}$ προκύπτει πως GRS = $\{(v_1\varphi(a_1),\dots,v_n\varphi(a_n)) \mid$ για κάθε $\varphi(\chi)$ που ανήκει στο $F_{k-1}[\chi]\}$.
Αυτό δικαιολογεί το ότι τα $a_1,\dots,a_n$ ονομάζονται εντοπισμοί του κώδικα

Ας δούμε κάτι ακόμα, έστω ένας πρωταρχικός γενικευμένος *GRS*, μήκους *n*, κώδικας επί ενός πεπερασμένου σώματος *F*, *q* το πλήθος στοιχείων. Υποθέτουμε πως $a_1, \dots, a_n$ είναι οι εντοπισμοί και $u_1, \dots, u_n$ οι συντελεστές στηλών του, τότε ένα διάνυσμα για τους συντελεστές στηλών του δυικού του κώδικα, *v*, είναι αυτό για το οποίο ισχύουν οι σχέσεις, $v_r = a_r/u_r$, $r = 1, \dots, n$. Για να το ελέγξουμε πηγαίνουμε στη σχέση η οποία αν ικανοποιείται, αυτό όντως είναι, δηλαδή στην $\sum_{r=1}^{n}(u_r v_r {a_r}^{(i+j)}) = 0$, για κάθε ζεύγος (*i*,*j*) με $0 \le i \le k-1$ και $0 \le j \le n-k-1$. Διαλέγουμε ένα τυχαίο ζεύγος (*i*,*j*), αντικαθιστώντας έχουμε $\sum_{r=1}^{n}(u_r\,(a_r/(u_r))\,{a_r}^{(i+j)}) = \sum_{r=1}^{n}(a_r {a_r}^{(i+j)}) = \sum_{r=1}^{q-1}(a_r {a_r}^{(i+j)})$, αφού $n = q-1$. Έστω *α* ένα πρωταρχικό στοιχείο του *F*, βλέπουμε ότι το σύνολο των εντοπισμών εξαντλεί τα μη μηδενικά στοιχεία του *F*. Άρα, για κάθε $r = 1, \dots, n$, θα υπάρχει φυσικός, l_r, με $1 \le l_r \le q-1$, όπου $a_r = \alpha^{l_r}$ και για κάθε αριθμό μεταξύ 1 και $q-1$ υπάρχει κάποιο l_r με το οποίο είναι ίσος. Έτσι το άθροισμα μας γίνεται $\sum_{r=1}^{q-1}(a_r {a_r}^{(i+j)}) = \sum_{r=1}^{q-1}(\,a^{l_r}(\alpha^{l_r})^{(i+j)}) = \sum_{r=1}^{q-1}(\,(\alpha^{i+j+1})^{l_r})$, επείδη με όσα είπαμε αν αναδιατάξουμε τα l_r σε αύξουσα σειρά προκύπτει η διάταξη 1, ... , $q-1$ το τελευταίο άθροισμα μπορεί να γραφτεί και ως $\sum_{p=1}^{q-1}(\alpha^{i+j+1})^p$. Η ταυτότητα
$\sum_{p=1}^{n}\beta^p = (\beta^{n+1} - \beta) / (\beta - 1)$ προφανώς ισχύει σε κάθε σώμα αν $\beta \ne 1$ (φαίνεται αμέσως). Άρα, βάζοντας στη θέση του β το α^{i+j+1}, όπου $\alpha^{i+j+1} \ne 1$ αφού
$0 \le i+j \le q-3$ κι άρα $1 \le i+j+1 \le q-2$,καταλήγουμε στη σχέση
$\sum_{p=1}^{q-1}(\,(\alpha^{i+j+1})^p) = ((\alpha^{i+j+1})^{n+1} - \alpha^{i+j+1}) / (\alpha^{i+j+1} - 1) =$
$((\alpha^{i+j+1})^q - \alpha^{i+j+1}) / (\alpha^{i+j+1} - 1) = 0.$

3.4 Μια βαθύτερη ματιά

Στις προηγούμενες παραγράφους εισάγαμε τους κώδικες BCH ως υποκώδικες των *CRS*. Αυτή η διαδικασία είναι, το λιγότερο, μη βολική για να βρούμε κάποιον BCH αν δε μας ενδιαφέρει ο κώδικας *CRS* από τον οποίο προέρχεται. Οπότε τώρα θα εξετάσουμε έναν ισοδύναμο τρόπο ορισμού τους που θα μας βοηθήσει στο να τους κατασκευάζουμε απευθείας.

Όπως είδαμε ένας *BCH* κώδικας επί ενός πεπερασμένου σώματος *F*, q πλήθους στοιχείων, κι ενός πρωταρχικού στοιχείου a μιας πεπερασμένης επέκτασης του *K* βαθμού *s* με q^s στοιχεία, είναι ο κώδικας που αποτελείται από τα διανύσματα του F^n, n $\leq q^s - 1$, οι συντεταγμένες των οποίων είναι οι συντελεστές των πολυωνύμων του $F_{n-1}[\chi]$ που ανάμεσα στις ρίζες τους είναι κι όλα τα στοιχεία $a^b,\ldots,a^{b+\delta-2}$, όπου $2 \leq \delta \leq n$ και $0 \leq b$. Έστω λοιπόν τώρα $\gamma(\chi)$ ένα πολυώνυμο που έχει για συντελεστή του μεγιστοβάθμιου όρου του τη μονάδα και με το μικρότερο βαθμό από τα αντικείμενα του $F_{n-1}[\chi]$ που ανάμεσα στις ρίζες τους είναι και τα στοιχεία $a^b,\ldots,a^{b+\delta-2}$. Οπότε αν πάρουμε τυχαία ένα άλλο πολυώνυμο του $F_{n-1}[\chi]$ το οποίο έχει ανάμεσα στις ρίζες του αυτά τα στοιχεία, έστω $\lambda(\chi)$, θα έχουμε από τον αλγόριθμο της διαίρεσης πως $\lambda(\chi) = \kappa(\chi) \cdot \gamma(\chi) + \upsilon(\chi)$ όπου ο βαθμός του $\upsilon(\chi)$ είναι μικρότερος του $\gamma(\chi)$. Από την προηγούμενη σχέση θα πρέπει τα $a^b,\ldots,a^{b+\delta-2}$ να είναι ρίζες και του $\upsilon(\chi)$, άτοπο, άρα $\upsilon(\chi) = 0$. Επομένως βλέπουμε ότι το $\gamma(\chi)$ είναι το μοναδικό πολυώνυμο του $F_{n-1}[\chi]$ με αυτές τις ιδιότητες κι ότι ο *BCH* κώδικας μας είναι ο πολυωνυμικός με πολυώνυμο γεννήτορα το $\gamma(\chi)$ και παραμέτρους $[n,\delta,a,b]$. Προφανώς όπως έχουμε πει είναι και υποώδικας του *CRS*$[n,\delta,a,b]$ επί του *K*.
Δηλαδή το $\gamma(\chi)$ θα μπορούσε να οριστεί ενναλακτικά και ως $\gamma(\chi) = \text{εκπ}(m_i(\chi), 1 \leq i \leq \delta - 1)$, όπου $m_i(\chi)$ είναι το μονικό πολυώνυμο του a^{b-1+i} πάνω από το *F*. Αυτή η ισοδυναμία στον Ορισμό του $\gamma(\chi)$ έπεται άμεσα από τον αλγόριθμο της διαίρεσης.

[5]<u>Θεώρημα</u>

Σε έναν *BCH*$[n,\delta,a,b]$ με γεννήτορα πολυώνυμο $\gamma(\chi)$, για την ελάχιστη απόσταση του *d*, ισχύει $\delta \leq d \leq \deg(\gamma(\chi)) + 1$.

<u>Απόδειξη</u>

Έχουμε ήδη δει ότι για ένα πολυωνυμικό κώδικα, η διάσταση του είναι όσο το μήκος του μείον τον βαθμό του πολυωνύμου που τον παράγει. Άρα η πρόταση έπεται από όσα έχουμε πει μέχρι τώρα.

∎

Το παραπάνω Θεώρημα [5] μπορεί να γενικευτεί και για μία κατηγορία πολυωνυμικών κωδίκων με διαδικασία κατασκευής παρόμοια με αυτή των *BCH*.

[6]<u>Θεώρημα</u>(Το φράγμα *BCH*)

Έστω *F* ένα πεπερασμένο σώμα, ω μια πρωταρχική *n*-οστή ρίζα της μονάδας και $2 \leq \delta \leq n$ και $0 \leq b$ φυσικοί. Έστω *C* ο κώδικας μήκους *n* που παράγεται από ένα πολυώνυμο $g(\chi)$ του $F[\chi]$ ώστε αυτό να έχει συντελεστή του μεγιστοβάθμιου όρου του τη μονάδα και τον ελάχιστο βαθμό από τα πολυώνυμα του $F[\chi]$ που ανάμεσα στις ρίζες τους έχουν τα $\omega^b,\ldots,\omega^{b+\delta-2}$. Τότε ο κώδικας είναι κυκλικός και για την ελάχιστη απόσταση του *d* ισχύει $\delta \leq d \leq \deg(g(\chi)) + 1$.

Απόδειξη

Το ότι ο κώδικας είναι κυκλικός προκύπτει από το γεγονός πως $(\omega^i)^n = (\omega^n)^i = 1$ για κάθε φυσικό *i*. Για τα υπόλοιπα αρκεί να παρατηρήσει κάποιος πως ο παρακάτω πίνακας είναι πίνακας ελέγχου ισοτιμίας για τον *C*

1	ω^b	…	$(\omega^b)^{n-1}$
1	ω^{b+1}	…	$(\omega^b)^{n-1}$
.	.	…	.
.	.	…	.
.	.	…	.
1	$\omega^{b+\delta-2}$	…	$(\omega^{b+\delta-2})^{n-1}$

οπότε σε συνδυασμό με ότι είπαμε πριν, το g(χ) είναι μοναδικό και υπόλοιπη απόδειξη είναι ίδια με αυτήν για τους *CRS* κώδικες.

■

Αν για ένα *BCH* κώδικα με παραμέτρους [*n*,*δ*,a,*b*] ισχύει ότι $b = 1$ τότε ο κώδικας λέγεται *υπό την στενή έννοια BCH*, γι αυτούς ισχύει το παρακάτω αποτέλεσμα.

[7]Πρόταση

Έστω *F* ένα σώμα με q το πλήθος στοιχεία. Έστω $n = q^s - 1$, $\delta = qt + 1$, $2 \leq \delta \leq n$. Πάντα μπορούμε να κατασκευάσουμε επί του *F* ένα *BCH* (υπό την στενή έννοια) κώδικα μήκους *n* και προσχεδιασμένης απόστασης *δ* με γεννήτορα πολυώνυμο γ(χ) το πολύ βαθμού $(q-1)ts$.

Απόδειξη

Όπως έχουμε πει και σε προηγούμενη απόδειξη υπάρχει επέκταση *K* του *F* βαθμού *s*. Έστω a πρωταρχικό της στοιχείο. Για κάθε $1 \leq i \leq \delta - 1 = qt$ έστω $m_i(\chi)$ μονικό πολυώνυμο του a^i επί του *F* και γ(χ) = εκπ($m_i(\chi)$, $1 \leq i \leq \delta - 1 = qt$). Από τον αλγόριθμο της διαίρεσης αποδεικνύεται ότι το γ(χ) είναι το πολυώνυμο γεννήτορας για τον *BCH*[*n*,*δ*,a,*b* = 1]. Κάθε $m_i(\chi)$ είναι βαθμού το πολύ *s* αφού η επέκταση *K* είναι βαθμού *s*. Άρα το γ(χ) θα έχει βαθμό το πολύ $(qt)s$. Για να ρίξουμε το άνω όριο για το βαθμό του γ(χ) παρατηρούμε ότι, $m_i(\chi) = m_{iq}(\chi)$. Αυτό ισχύει διότι ένα πολυώνυμο του *F*[χ] έχει για ρίζα το a^i, αν και μόνο αν, έχει για ρίζα το $(a^i)^q = a^{iq}$. Ο λόγος για τον οποίο ισχύει κάτι τέτοιο εξηγείται στα σχόλια που ακολουθούν το Θεώρημα[42] του Κεφαλαίου 2. Επομένως τα πολυώνυμα $m_q, m_{2q}, \ldots, m_{tq}$ μπορούμε να μη τα λάβουμε υπόψη στον υπολογισμό του εκπ και το θεώρημα αποδείχθηκε.

■

Στη περίπτωση που ένας *BCH* κώδικας επί ενός πεπερασμένου σώματος *F*, q στο πλήθος στοιχείων κι ενός πρωταρχικού στοιχείου a, μιας πεπερασμένης επέκτασης του *K* βαθμού *s* με q^s στοιχεία, έχει μήκος $n = q^s - 1$, τότε ονομάζεται *πρωταρχικός*. Ένας

πρωταρχικός *BCH* είναι κυκλικός με τη δικαιολόγηση που δόθηκε και για τους πρωταρχικούς *CRS*. Αν επιπλέον η επέκταση του *K* έχει βαθμό 1, δηλαδή *K* = *F* με αποτέλεσμα *n* = *q* – 1, τότε ονομάζεται *κώδικας Reed-Solomon*.

Έστω *RS*[*n*,*k*,*n* – *k* + 1] ένας πρωταρχικός συμβατικός κώδικας Reed – Solomon ενός πεπερασμένου σώματος *F*, δηλαδή ένας κώδικας Reed-Solomon. Όπως είπαμε αυτός είναι ειδική περίπτωση ενός πρωταρχικού *GRS* με στοιχεία εντοπισμού $a_i = a^{i-1}$ και συντελεστές στηλών $u_i = a^{i-1}$. Απο τα προηγούμενα ο δυικός του κώδικας θα έχει πίνακα συντελεστών $v_r = a_r/u_r$, *r* = 1, … ,*n* , δηλαδή $v_r = a^{i-1}/a^{i-1} = 1$.

Συνεπώς, *RS* = {$\varphi(1),\varphi(\alpha)$, ... ,$\varphi(\alpha^{n-1})$ | για κάθε $\varphi(\chi)$ στο $F_{k-1}[\chi]$ }. Αυτή η έκφραση αποτέλεσε ιστορικά τον πρώτο ορισμό κωδίκων της κατηγορίας Reed – Solomon, το σημαντικότερο όμως είναι ότι αποτελεί το πρώτο βήμα για την εισαγωγή στην περιοχή των μαθηματικών που ονομάζεται <<Αλγεβρική Γεωμετρία και κώδικες>> που αποτελεί πεδίο σύγχρονης έρευνας.

Παρακάτω θα δώσουμε ένα παράδειγμα τέτοιου κώδικα όμως πριν από αυτό θα πούμε δύο λόγια για τους πίνακες *ισοτιμίας* των *BCH*.

Αν

$$P = \begin{matrix} 1 & a^b & \dots & (a^b)^{n-1} \\ 1 & a^{b+1} & \dots & (a^{b+1})^{n-1} \\ . & . & \dots & . \\ . & . & \dots & . \\ . & . & \dots & . \\ 1 & a^{b+\delta-2} & \dots & (a^{b+\delta-2})^{n-1} \end{matrix}$$

Τότε ξέρουμε πως ένα διάνυσμα *c* του F^n ανήκει στον *BCH*[*n*,*δ*,a,*b*] αν και μόνο αν
c · *P** = 0, όμως ο *P* δεν είναι πίνακας ισοτιμίας για τον κώδικα διότι τα στοιχεία του δεν είναι στοιχεία του *F*. Παρόλα αυτά μπορούμε να χρησιμοποιήσουμε αυτή την ιδιότητα του *P* για να κατασκευάσουμε ένα πίνακα ισοτιμίας του κώδικα μας. Τα στοιχεία του *P* προέρχονται από το σύνολο *K* το οποίο είναι διανυσματικός χώρος διάστασης s πάνω από το *F* και έστω *B* = $\{e_1,\dots,e_s\}$ μια βάση του. Συμβολίζουμε με [*r*(i,j)] τον πίνακα στήλη (*s* × 1) που έχει για στοιχεία τους συντελεστές *F* που αντιστοιχούν στο γραμμικό συνδυασμό των στοιχείων της *B* που μας δίνουν το στοιχείο *p*(*i*,*j*) που βρίσκεται στην (*i*,*j*) θέση του πίνακα *P*. Αν απομονώσουμε τώρα μια γραμμή *i* του *P* θα δούμε ότι, όπως προείπαμε ένα στοιχείο *c* του F^n ανήκει στον *BCH*[*n*,*δ*,a,*b*] αν και μόνο αν *c* · *P** = 0 που είναι ισοδύναμο με *P* · *c** = 0 δηλαδή αν
c = ($c_0,\dots,c_{n-1}$) με $p(i,0)c_0 + \dots + p(i,(n-1))c_{n-1} = 0$ που κι αυτό με τη σειρά του είναι ισοδύναμο με $[r(i,0)]c_0 + \dots + [r(i,(n-1))]c_{n-1} = 0$ διότι αυτό που θα πάρουμε τώρα θα είναι ένας πίνακας στήλη (*s* × 1) που είναι οι συντελεστές των στοιχείων της βάση *B* που μας δίνουν το μηδενικό στοιχείο, άρα πρέπει όλοι να είναι μηδέν. Επομένως αποδείξαμε ότι ο παρακάτω ((*δ* – 1)*s* × *n*) *R* πίνακας, είναι ένας πίνακας ελέγχου ισοτιμίας για τον BCH[*n*,*δ*,a,*b*].

$$R = \begin{matrix} [r(0,0)] & [r(0,1)] & \dots & [r(0,(n-1))] \\ [r(1,0)] & [r(1,1)] & \dots & [r(1,(n-1))] \\ . & . & \dots & . \\ . & . & \dots & . \\ . & . & \dots & . \\ [r((\delta-2),0)] & [r((\delta-2),1)] & \dots & [r((\delta-2),(n-1))] \end{matrix}$$

3.5 Παραδείγματα

Παράδειγμα 1

Για να κατασκευάσουμε ένα πίνακα *BCH* δεν χρειάζεται να βρούμε τον πίνακα ισοτιμίας του, αρκεί να προσδιορίσουμε το πολυώνυμο γεννήτορας του.
Θέλουμε να κατασκευάσουμε ένα πίνακα Reed-Solomon που να διορθώνει μέχρι 4 λάθη. Συνήθως δεν συναντώνται περισσότερα στις περισσότερες εφαρμογές. Θυμόμαστε ότι τέτοιου είδους κώδικας είναι ένας πρωταρχικός κώδικας του οποίου η επέκταση είναι βαθμού 1. Επιπλέον από το Θεώρημα[11] του Κεφαλαίου 1 ένας κώδικας για να επιτυγχάνει διόρθωση τεσσάρων στο πλήθος λαθών πρέπει η ελάχιστη απόσταση του να είναι τουλάχιστον 9. Οπότε παίρνουμε $\delta = 10$, $n = 12$ και $b = 1$ κι διαλέγουμε ένα σώμα με 13 στοιχεία. Όπως έχουμε αναφέρει ήδη, υπάρχει μία μόνο δομή σώματος με τόσα το πλήθος στοιχεία κι εμείς παίρνουμε την πιο οικεία μορφή της που είναι το Z_{13}. Οπότε ψάχνουμε ένα πρωταρχικό στοιχείο του Z_{13} (θα μπορούσαμε να είχαμε διαλέξει να εργαστούμε στο Z_{11} αλλά τότε η διάσταση του κώδικα μας θα ήταν 1 και δεν θα είχαμε πολλές κωδικολέξεις). Το 2 είναι ένα τέτοιο, ένας απλός υπολογισμός θα μας πείσει. Υπολογίζουμε τώρα τα a^b,…,$a^{b+\delta-2}$ τα οποία είναι τα 2,4,8,3,6,12,11,9,5. Αφού τώρα η επέκταση μας ήταν βαθμού 1 το ελάχιστο μονικό πολυώνυμο που ψάχνουμε είναι το $f(\chi) = (\chi - 2)\dots(\chi - 5)$, οπότε ο κώδικας μας έχει διάσταση 3 και είναι αυτός που παράγεται από το $f(\chi)$. Αν θέλουμε να βρούμε μία βάση για το κώδικας μας αρκεί να πολλαπλασιάσουμε το $f(\chi)$ με τα $1,\chi,\chi^2$ αφού αυτά είναι βάση του $(Z_{13})_2[\chi]$, και να δούμε ποιους συντελεστές θα δώσουν. Κάνουμε τις πράξεις και βρίσκουμε ότι το $f(\chi)$ ισούται με

$f(\chi) = \chi^9 - 8\chi^8 + 3\chi^7 - 3\chi^6 + 6\chi^5 - 3\chi^4 + 9\chi^3 - 8\chi^2 + 6\chi - 5$ άρα ένας πίνακας γεννήτορας για τον κώδικα μας είναι ο ακόλουθος T

$$T = \begin{matrix} -5 & 6 & -8 & 9 & -3 & 6 & -3 & 3 & -8 & 1 & 0 & 0 \\ 0 & -5 & 6 & -8 & 9 & -3 & 6 & -3 & 3 & -8 & 1 & 0 \\ 0 & 0 & -5 & 6 & -8 & 9 & -3 & 6 & -3 & 3 & -8 & 1 \end{matrix}$$

και άρα κατασκευάσαμε ένα κυκλικό (όπως έχουμε ήδη εξηγήσει) κώδικα με 13^3 κωδικολέξεις μήκους 12 που διορθώνει μέχρι 4 λάθη, δηλαδή έχουμε μια αναλογία 1/3 μεταξύ των ανεκτών λαθών και το μήκος του κώδικα που είναι αρκετά ικανοποιητική.

Παράδειγμα 2

Θα κατασκευάσουμε ένα *CRS* ικανό να διορθώνει μέχρι 5 λάθη. Όπως ξέρουμε θα πρέπει να έχει ελάχιστη απόσταση, *d*, τουλάχιστον 11. Στους *CRS*(*n*,*δ*,a,*b*) ισχύει $d = \delta$, οπότε καθορίζουμε $\delta = 11$, επίσης είναι γνωστό πως $n - \delta + 1$ θα είναι η διάσταση του κώδικα. Για να έχουμε αρκετές κωδικολέξεις ας διαλέξουμε ο κώδικας μας να έχει διάσταση 4, άρα $n - \delta = 3$. Το μόνο που θέλουμε τώρα είναι να βρούμε ένα σώμα, *K*, με τουλάχιστον $n + 1 = 15$ στοιχεία. Θα πάρουμε το Z_2 και θα κατασκευάσουμε επέκταση του βαθμού 4, αφού $2^4 = 16 > 15$. Το πολυώνυμο $\chi^4 + \chi + 1$ δεν έχει ρίζα στο Z_2 και είναι ανάγωγο (εύκολα αποδυκνείεται με έλεγχο όλων των περιπτώσεων). Οπότε, από Θ.Kronecker, $K = Z_2[\chi] / <\chi^4 + \chi + 1>$. Αυτό που θέλουμε να κάνουμε τώρα είναι να βρούμε ένα πρωταρχικό στοιχείο του *K*. Για κάθε στοιχείο φ στο *K* από
Θ. Lagrange ισχύει $\varphi^{2^4-1} = \varphi^{15} = 1$. Οπότε αφού $15 = 3 \cdot 5$ αν φ στοιχείο του K και φ^3, φ^5 διαφορετικά της μονάδας, το φ είναι πρωταρχικό του *K*. Θα κάνουμε τον έλεγχο για το αντικείμενο $a = \chi + <\chi^4 + \chi + 1>$. Αμέσως βλέπουμε ότι $a^3 \neq 1$, αφού $\{1,a,a^2,a^3\}$ βάση του *K*. Για να ελέγξουμε και την άλλη περίπτωση παρατηρούμε ότι $a^5 = a^4\, a = -a + (-a^2) \neq 1$ για τον ίδιο λόγο με πριν. Άρα το a είναι πρωταρχικό στοιχείο του *K*. Για ευκολία παίρνουμε $b = 1$ οπότε το πολυώνυμο γεννήτορας $\gamma(\chi)$ του κώδικα μας είναι το $\gamma(\chi) = (\chi - a) \ldots (\chi - a^{10})$. Ο πίνακας ισοτιμίας του κώδικα μας θα είναι ο T

$$T = \begin{matrix} 1 & a & \ldots & a^{13} \\ 1 & a^2 & \ldots & (a^2)^{13} \\ . & . & \ldots & . \\ . & . & \ldots & . \\ . & . & \ldots & . \\ 1 & a^{10} & \ldots & (a^{10})^{13} \end{matrix}$$

Δηλαδή ο κώδικας μας είναι ο *CRS*[14,11,a,1] = { τα διανύσματα $(c_0, \ldots, c_{13})$ του K^{13} | το $c_0 + c_1\chi + \ldots + c_{13}\chi^{13}$ έχει όλα τα a, ... , a^{10}ως ρίζες }. Όπότε τώρα κατασκευάσαμε κώδικα με 4^{16} στοιχεία, μήκους 14, που διορθώνει μέχρι 5 λάθη. Εδώ η αναλογία ανεκτών λαθών/μήκος είναι καλύτερη από 1/3.

3.6 Εναλλασόμενοι Κώδικες

Όπως είδαμε και παραπάνω, τους *BCH* κώδικες τους πήραμε ως τη τομή ενός συμβατικού κώδικα Reed-Solomon με το σώμα *F* από το οποίο ξεκινήσαμε. Εδώ θα κάνουμε το ίδιο μόνο που στη θέση των συμβατικών Reed-Solomon θα έχουμε τους γενικευμένους Reed-Solomon. Λόγο αυτής της ομοιότητας στη κατασκευή οι αποδείξεις είναι σχετικά ίδιες. Θα δούμε ότι με αυτή τη διαδικασία θα καταλήξουμε στους κώδικες Goppa. Ξεκινώντας έχουμε πάλι ένα σώμα *F*, *q* το πλήθος στοιχείων, και *K* μια επέκταση του βαθμού s. Κατασκευάζουμε τώρα ένα κώδικα *GRS*[*n*, *k*, $d = n - k + 1$] επί του *K* με τον τρόπο που έχουμε αναφέρει. Τότε όπως

προηγουμένος ο κώδικας $A = GRS \cap F^n$ θα είναι ένας γραμμικός κώδικας επί του F με ελάχιστη απόσταση τουλάχιστον d. Το ζεύγος αυτών των δύο κωδίκων ονομάζεται ζεύγος εναλλασσόμενων κωδίκων και ο καθένας μεμονωμένα εναλλακτικός (ως προς τον άλλον) κώδικας. Προφανώς αν H είναι ο πίνακας ισοτιμίας για τον κώδικα GRS για να πάρουμε ένα πίνακα ισοτιμίας για τον κώδικα A κάνουμε την εντελώς όμοια διαδικασία που περιγράψαμε και για τους BCH. Καταλήγουμε έτσι με ένα πίνακα R $((d-1)s \times n)$, αφού $\delta = d$ όπου

$$R = \begin{matrix} [r(0,0)] & [r(0,1)] & \dots & [r(0,(n-1))] \\ [r(1,0)] & [r(1,1)] & \dots & [r(1,(n-1))] \\ . & . & \dots & . \\ . & . & \dots & . \\ . & . & \dots & . \\ [r((\delta-2),0)] & [r((\delta-2),1)] & \dots & [r((\delta-2),(n-1))] \end{matrix}$$

Από εδώ φαίνεται ότι για την διάσταση λ του A ισχύει $n - \lambda \leq (d-1)s$.
Αυτό ισχύει επειδή γνωρίζουμε πως για ένα πίνακα ισοτιμίας ενός γραμμικού κώδικα, οι γραμμές του είναι στοιχεία του δυικού υποχώρου του που περιέχουν και μια βάση του δυικού. Δηλαδή θα έχουμε $n - (d-1)s \leq \lambda$ που είναι ένα κάτω φράγμα για τη διάσταση του A και άρα και για το πλήθος των κωδικών λέξεων που περιέχει. Επομένως αν ρυθμίσουμε τις παραμέτρους $n,\delta,$ που αυτές καθορίζουν και τις d,s , μπορούμε να καταλήξουμε σε επιθυμητή διάσταση, αρκεί να μη ξεχνάμε πως παράλληλα θα πρέπει $n \leq q^s - 1$.

3.7 Goppa

Σε αυτό το σημείο είμαστε έτοιμοι να εισάγουμε τους κώδικες Goppa, η όποια δυσκολία βρίσκεται στον ορισμό τους αφού τα αποτελέσματα γι αυτούς θα έπονται από ότι έχουμε πει μέχρι τώρα. Έστω F ένα πεπερασμένο σώμα με q το πλήθος στοιχεία και K μια επέκταση του βαθμού m(όπως έχουμε δει ο βαθμός μπορεί να είναι όποιος φυσικός επιθυμούμε). Έστω $g(\chi)$ στοιχείο του $K[\chi]$ και $R_{g(\chi)}[\chi] := K[\chi]/\langle g(\chi)\rangle$ η ακέραια περιοχή των υπολοίπων. Κάθε στοιχείο της $R_{g(\chi)}[\chi]$, $\varphi(\chi) + \langle g(\chi)\rangle$ θα το συμβολίζουμε με $\varphi(\chi)^{\vdash}$. Όπως είδαμε από τα Θεωρήματα[37],[39] του Κεφαλαίου 2 αν το $g(\chi)$ δεν είναι ανάγωγο η $R_{g(\chi)}[\chi]$ δεν είναι σώμα. Παρ' όλα αυτά για ένα στοιχείο a του K όπου $g(a) \neq 0$ θα έχουμε από τον αλγόριθμο της διαίρεσης πως
$g(\chi) = \kappa(\chi)(\chi - a) + g(a)$ άρα
$g(a)^{-1}g(\chi) = g(a)^{-1}\kappa(\chi)(\chi - a) + 1$ ή
$(- g(a)^{-1})\kappa(\chi)(\chi - a) = 1 + (- g(a)^{-1})\, g(\chi)$
δηλαδή το $(\chi - a)^{\vdash}$ έχει αντίστροφο και
$((\chi - a)^{\vdash})^{-1} = (\,(g(\chi) - g(a)) / (\chi - a)\,)\,(-g(a)^{-1})\,)^{\vdash}$. Αυτό ισχύει αφού
$g(\chi) - g(a) = \kappa(\chi)(\chi - a)$ οπότε $g(a)^{-1}(g(\chi) - g(a)) = g(a)^{-1}\kappa(\chi)(\chi - a)$ κι άρα
$(\,(g(\chi) - g(a))\, g(a)^{-1}\,) / (\chi - a) = g(a)^{-1}\kappa(\chi)$

[8]Ορισμός

Έστω *F* ένα σώμα με *q* το πλήθος στοιχεία, *K* μία επέκταση του βαθμού *m* και $L = \{a_1,\ldots,a_n\}$ υποσύνολο του *K*. Έστω $g(\chi)$ στοιχείο του $K[\chi]$ με $2 \le \deg(g(\chi)) \le v < n$ και με την ιδιότητα $g(a_i) \neq 0$ για κάθε στοιχείο του *L*. Το σύνολο $G(L,g(\chi)) = \{c = (c_1 \ldots c_n) \mid c_i$ στοιχεία του *F* και $\sum_{i=1}^{n}(c_i^{\ulcorner} /(\chi - a_i)^{\ulcorner}) = 0\}$ θα ονομάζεται *κώδικας Goppa*.

Όπως είδαμε ένας κώδικας Goppa έχει δύο ορίσματα, το *L* θα λέγεται σύνολο εντοπισμού του κώδικα και το $g(\chi)$ πολυώνυμο γεννήτορας του κώδικα. Για να δείξουμε ότι είναι υποκώδικες των γενικευμένων Reed – Solomon, θα αναλύσουμε το στοιχείο $((\chi - a_i)^{\ulcorner})^{-1}$ χρησιμοποιώντας των αλγόριθμο της διαίρεσης και τη σχέση $((\chi - a_i)^{\ulcorner})^{-1} = (((g(\chi) - g(a)) / (\chi - a))(-g(a)^{-1}))^{\ulcorner}$.

Έστω

$g(\chi) = r_v\chi^v + r_{v-1}\chi^{v-1} + \ldots + r_0$.

Από εδώ βλέπουμε πως $(g(\chi) - g(a)) / (\chi - a) =$

$r_v\chi^{v-1} + (r_{v-1} + ar_v)\chi^{v-2} + (r_{v-2} + a(r_{v-1} + ar_v))\chi^{v-3} + \ldots +$

$+ (r_1 + a(r_2 + a(r_3 + \ldots + a(r_{v-1} + ar_v))))\ldots)$. Ο σταθερός όρος μπορεί να γραφτεί και στη μορφή $r_1 + \ldots + a^{v-1}r_v$. Πηγαίνοντας πίσω στη σχέση ορισμού του κώδικα βλέπουμε πως ένα στοιχείο *c* ανήκει στον κώδικα αν και μόνο αν

$\sum_{i=1}^{n}[c_i\, g(a_i)^{-1}\,(r_v\chi^{v-1} + (r_{v-1} + a_ir_v)\chi^{v-2} + \cdots + (r_1 + \cdots + a_i{}^{v-1}r_v))\,]^{\ulcorner} = 0^{\ulcorner}$. Επειδή $0^{\ulcorner} = \langle g(\chi)\rangle$ κι άρα κάθε στοιχείο εκεί μη μηδενικό είναι βαθμού τουλάχιστον *v*. Το άθροισμα αυτό, αν το δούμε σε επίπεδο αντιπροσώπων των συμπλόκων, θα είναι ένα $(v - 1)$ βαθμού πολυώνυμο το οποίο θα πρέπει να ανήκει στο $\langle g(\chi)\rangle$. Άρα από τα προηγούμενα κάθε συντελεστής των όρων του θα πρέπει να είναι μηδέν. Οπότε μας προκύπτουν *v* εξισώσεις. Υπολογίζουμε τους συντελεστές με φθίνουσα σειρά ως προς τους δείκτες τους και βλέπουμε πως

$\sum_{i=1}^{n}[c_i\, g(a_i)^{-1}r_v\,] = 0$

$\sum_{i=1}^{n}[\, c_ig(a_i)^{-1}\,(r_{v-1} + a_ir_v)\,] = 0$

$\sum_{i=1}^{n}[\, c_ig(a_i)^{-1}\,(r_{v-2} + a_i(r_{v-1} + a_ir_v\,)\,)\,] = 0$

.
.
.

$\sum_{i=1}^{n}[\, c_i\, g(a_i)^{-1}\,(r_0 + \cdots + a_i{}^{v-1}r_v\,)\,] = 0$

Από την πρώτη σχέση τώρα εξάγουμε για την δεύτερη πως $\sum_{i=1}^{n}[\, c_i g(a_i)^{-1} a_i \,] = 0$, διότι $r_\nu \neq 0$. Από αυτήν την σχέση τώρα και την πρώτη από τις προηγούμενες εξάγουμε για την τρίτη από αυτές πως $\sum_{i=1}^{n}[\, c_i g(a_i)^{-1} a_i^{\,2} \,] = 0$, από αυτές τις δύο τώρα και την πρώτη από τις προηγούμενες συνεχίζοντας όμοια καταλήγουμε στην $\sum_{i=1}^{n}[\, c_i g(a_i)^{-1} a_i^{\,\nu-1} \,] = 0$.

Αν εκφράσουμε αυτέ τις σχέσεις με πίνακες έχουμε ότι η *c* ανήκει στον $G(L,g(\chi))$ αν,
$c \cdot H^* = H \cdot c^* = 0$, όπου $H = \Gamma \cdot \Delta$ με

$$\Gamma = \begin{matrix} 1 & 1 & \dots & 1 \\ a_1 & a_2 & \dots & a_n \\ . & . & \dots & . \\ . & . & \dots & . \\ . & . & \dots & . \\ a_1^{\nu-1} & a_2^{\nu-1} & \dots & a_n^{\nu-1} \end{matrix}$$

και

$$\Delta = \begin{matrix} g(a_1)^{-1} & 0 & \dots & 0 \\ 0 & g(a_2)^{-1} & \dots & 0 \\ . & . & \dots & . \\ . & . & \dots & . \\ . & . & \dots & . \\ 0 & 0 & \dots & g(a_n)^{-1} \end{matrix}$$

Αυτό το αποτέλεσμα σε συνδυασμό με τα προηγούμενα αποδεικνύουν το παρακάτω Θεώρημα.

[9]<u>Θεώρημα</u>
Έστω *F* ένα πεπερασμένο σώμα με *q* στοιχεία. *K* μια επέκταση του βαθμού *m* και $L = \{a_1,\dots,a_n\}$ ένα υποσύνολο του *K*. Έστω $g(\chi)$ στοιχείο του $K[\chi]$ με $2 \leq \deg(g(\chi)) \leq \nu < n$ και με την ιδιότητα $g(a_i) \neq 0$ για κάθε *i*. Έστω ο *GRS* κώδικας επί του *K* με πίνακα ισοτιμίας $H = \Gamma \cdot \Delta$, όπου

$$\Gamma = \begin{matrix} 1 & 1 & \dots & 1 \\ a_1 & a_2 & \dots & a_n \\ . & . & \dots & . \\ . & . & \dots & . \\ . & . & \dots & . \\ a_1^{\nu-1} & a_2^{\nu-1} & \dots & a_n^{\nu-1} \end{matrix}$$

και

$$\Delta = \begin{matrix} g(a_1)^{-1} & 0 & \dots & 0 \\ 0 & g(a_2)^{-1} & \dots & 0 \\ . & . & \dots & . \\ . & . & \dots & . \\ . & . & \dots & . \\ 0 & 0 & \dots & g(a_n)^{-1} \end{matrix}$$

τότε ο εναλλακτικός κώδικας $A = GRS \cap F^n$ είναι ο κώδικας Goppa $G(L,g(\chi))$ με παραμέτρους $[n,k,d]$ για τις οποίες ισχύει $v + 1 \leq d$, $n - mv \leq k \leq n - v$.

Απόδειξη
Έχει προηγηθεί μαζί με τα αποτελέσματα που είπαμε για τους εναλλασσόμενους κώδικες.

■

3.8 Εφαρμογές

Οι κώδικες Reed – Solomon είναι ιδιαίτερα αποτελεσματικοί όταν πρόκειται για διόρθωση σφαλμάτων τα οποία βρίσκονται σε διαδοχικές θέσεις. Λόγο αυτού του γεγονότος είχαν χρησιμοποιηθεί για τη μετάδοση μηνυμάτων στο διάστημα όπου ύστερα από εμπειρικά δεδομένα είχε διαπιστωθεί ότι τα σφάλματα συμβαίνουν ακριβώς με αυτόν τον τρόπο, δηλαδή σε ομάδες ακολουθιών. Για τον ίδιο λόγο χρησιμοποιήθηκαν και στα CD.

Βιβλιογραφία

[1] Δημήτριος Α. Βάρσος <<Μια Εισαγωγή στην αλγεβρική θεωρία Κωδίκων>> .

[2] John B. Fraleigh <<Εισαγωγή στην Άλγεβρα>>.

[3] Gilbert Strang <<Γραμμική άλγεβρα κι εφαρμογές>>.

[4] Ανάργυρος Γ. Φελλούρης <<Γραμμική Άλγεβρα και Αναλυτική Γεωμετρία>>.

[5] Paul R. Halmos <<Αφελής Συνολοθεωρία>>

[6] Κοντογεώργης Α., Αντωνιάδης Ι. <<Πεπερασμένα Σώματα και Κρυπτογραφία>>.

[7] Χ. Κουκουβίνος, Α. Παπαϊωάνου <<Θεωρία Πληροφοριών και Κωδίκων>>.