Τμήμα Μαθηματικών
Πανεπιστήμιο Κρήτης

Εύρεση και αποκωδικοποίηση βέλτιστων κωδίκων με χρήση Πεπερασμένης Γεωμετρίας και Βάσεων Gröbner

ΜΕΤΑΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Μάριος Μαγιολαδίτης

Ηράκλειο 2004

Η μεταπτυχιακή αυτή εργασία κατατέθηκε στο Τμήμα Μαθηματικών του Πανεπιστημίου Κρήτης τον Οκτώβρη του 2004. Επιβλέπων ήταν ο καθηγητής Γιάννης Α. Αντωνιάδης.

Την επιτροπή αξιολόγησης αποτέλεσαν οι: Γιάννης Αντωνιάδης, Θεόδουλος Γαρεφαλλάκης και Νίκος Τζανάκης.

Η εργασία βρίσκεται σε ηλεκτρονική μορφή στην διεύθυνση:
http://www.math.uoc.gr/~marios

Τελευταία διόρθωση: 19/11/2004

Εισαγωγή

Η μετάδοση και η μεταφορά μηνυμάτων μέσω καναλιών είναι ένα σημαντικό πρακτικό πρόβλημα. Η θεωρία κωδικοποίησης ασχολείται με την εύρεση μεθόδων που ελαχιστοποιούν την πιθανότητα λάθους στην μετάδοση ενός μηνύματος.

Η εξάπλωση της χρήσης ηλεκτρονικών υπολογιστών μετά την δεκαετία του 1950 έπαιξε τον καθοριστικότερο ρόλο στην ανάπτυξη των λεγόμενων κωδίκων διόρθωσης λαθών (error-correcting codes), κωδίκων, δηλαδή, που θα ανιχνεύουν και θα διορθώνουν λάθη που έχουν προκύψει κατά την μεταφορά μηνυμάτων. Η ανάπτυξη της αντίστοιχης θεωρίας οφείλεται κυρίως στους Shannon και Hamming.

Ο Hamming είχε πρόσβαση σε έναν από τους πρώτους ηλεκτρονικούς υπολογιστές αλλά βρίσκονταν σε χαμηλή προτεραιότητα στη λίστα των χρηστών. Η διαδικασία που ακολουθούσε ήταν η εξής: Εισήγαγε δεδομένα στον υπολογιστή κωδικοποιημένα πάνω σε χαρτί μηχανής κάθε Παρασκευή και έπαιρνε τα αποτελέσματά του την Δευτέρα. Πολλές φορές έκανε λάθος στην εισαγωγή των δεδομένων με αποτέλεσμα ο υπολογιστής να μην μπορεί να δώσει αποτέλεσμα και να περιμένει ξανά μέχρι την επόμενη Παρασκευή για να δώσει ξανά τα δεδομένα του. Η ιδέα του Hamming ήταν ότι αν ο υπολογιστής μπορεί να βρει ένα λάθος γιατί να μην μπορεί και να το διορθώσει; Σκέφτηκε επομένως το ακόλουθο μοντέλο.

Ο υπολογιστής του Hamming έπαιρνε δεδομένα σε εφτάδες που αποτελούνται από 0 και 1. Θεωρούμε μια εφτάδα $c_1c_2c_3c_4c_5c_6c_7$ (όπου $c_i = 0$ ή 1) η οποία θέλουμε να είναι αποδεκτή από τον υπολογιστή. Ο Hamming σκέφτηκε τα c_i να ικανοποιούν τις ακόλουθες εξισώσεις mod 2:

$$c_1 + c_3 + c_5 + c_7 = 0$$
$$c_2 + c_3 + c_6 + c_7 = 0$$
$$c_4 + c_5 + c_6 + c_7 = 0$$

Τα c_3, c_5, c_6, c_7 επιλέγονται ελεύθερα και τα c_1, c_2, c_4 προκύπτουν από τις εξισώσεις. Οι εφτάδες που θα ικανοποιούν τις παραπάνω συνθήκες θα είναι αποδεκτές από τον υπολογιστή και ονομάζονται κωδικές λέξεις. Οι υπόλοιπες όχι. Αν υποθέσουμε ότι το τελικά ο υπολογιστής έλαβε το $x_1x_2x_3x_4x_5x_6x_7$ σχηματίζουμε τις ακόλουθες εξισώσεις mod 2:

$$z_1 = x_1 + x_3 + x_5 + x_7$$
$$z_2 = x_2 + x_3 + x_6 + x_7$$
$$z_4 = x_4 + x_5 + x_6 + x_7$$

Αν το $x_1x_2x_3x_4x_5x_6x_7$ είναι μια κωδική λέξη τότε $z_1 = z_2 = z_4 = 0$. Αν υπάρχει ακριβώς ένα λάθος τότε ακριβώς ένα από τα z_1, z_2, z_4 είναι διαφορετικό από το μηδέν και το λάθος βρίσκεται στην θέση $z_1 + 2z_2 + 4z_3$ (χρησιμοποιώντας κανονική πρόσθεση και όχι πρόσθεση mod 2). Έτσι δημιουργήθηκε ο πρώτος κώδικας διόρθωσης λαθών.

Ένας κώδικας αποτελείται από 3 βασικές παραμέτρους. Το πλήθος M των κωδικών του λέξεων, το μήκος n των κωδικών λέξεων και την ελάχιστη απόσταση d μεταξύ

τους. Είναι σημαντικό να κατασκευάζουμε κώδικες οι οποίοι θα έχουν μεγάλο M και μικρό n για οικονομία στην μετάδοση του μηνύματος αλλά και μεγάλο d ώστε να μπορούμε να διορθώνουμε όσο το δυνατόν περισσότερα λάθη.

Βασικός σκοπός της εργασίας είναι η εύρεση γραμμικών κωδίκων που μια από τις τρεις παραμέτρους, δοσμένων των άλλων δύο, είναι βέλτιστη. Αυτά τα προβλήματα ονομάζονται κεντρικά προβλήματα της Θεωρίας Κωδικοποίησης.

Στο πρώτο κεφάλαιο εισάγουμε τον αναγνώστη σε βασικές έννοιες από την θεωρία της Κωδικοποίησης, των Πεπερασμένων Γεωμετριών. Κάνουμε μια σύνοψη βασικών προτάσεων που θα μας φανούν χρήσιμες στα επόμενα κεφάλαια.

Στο δεύτερο κεφάλαιο συνδέουμε το πρόβλημα της εύρεσης του μέγιστου n, δοσμένων των n – k, d και q, για το οποίο υπάρχει ένας $[n, k, d]_q$-κώδικας με ένα άλλο γνωστό πρόβλημα: το πεπερασμένο packing πρόβλημα, αυτό της εύρεσης του μεγαλύτερου n για το οποίο υπάρχει σύνολο που αποτελείται από n στοιχεία τα οποία είναι ανά d – 1 γραμμικά ανεξάρτητα. Το πρόβλημα αυτό αν και λύθηκε γρήγορα για τις περιπτώσεις όπου $d \leq 3$ παραμένει ανοικτό μέχρι σήμερα. Χρησιμοποιούμε Πεπερασμένη Γεωμετρία για να αντιμετωπίσουμε το πρόβλημα και παρουσιάζουμε όλα τα γνωστά αποτελέσματα μέχρι σήμερα. Επίσης, παρουσιάζουμε συνοπτικά την εξέλιξη των αποτελεσμάτων στην περίπτωση των MDS κωδίκων (κώδικες για τους οποίους ισχύει $d = k + 1$), την περίφημη βασική εικασία για τους MDS κώδικες.

Στο τρίτο κεφάλαιο επιχειρούμε μια άλλη προσέγγιση του προβλήματος αυτό της εύρεσης του ελάχιστου n δοσμένων των k, d και q, για το οποίο υπάρχει ένας $[n, k, d]_q$-κώδικας. Δείχνουμε ότι ένα πολύ γνωστό φράγμα της Θεωρίας Κωδικοποίησης, το φράγμα του Griesmer μαζί με ένα άλλο γνωστό αποτέλεσμα μετατρέπουν το πρόβλημα μας σε ένα πεπερασμένο πρόβλημα. Παρουσιάζουμε όλα τα γνωστά αποτελέσματα στην περίπτωση των τετραδικών κωδίκων (κώδικες με $q = 4$) και τα πρόσφατα αποτελέσματα στην περίπτωση των δυαδικών κωδίκων.

Στο τέταρτο κεφάλαιο χρησιμοποιούμε την Θεωρία των Βάσεων Gröbner για να παρουσιάσουμε ένα αλγόριθμο αποκωδικοποίησης κυκλικών κωδίκων. Αρχικά εισάγουμε βασικές έννοιες της θεωρίας και στη συνέχεια παρουσιάζουμε εφαρμογές της στην αποκωδικοποίηση. Αποδεικνύεται ότι ο αλγόριθμος που παρουσιάζουμε γενικεύεται για όλους τους γραμμικούς κώδικες.

Ευχαριστίες

Θα ήθελα να ευχαριστήσω τον καθηγητή μου Γιάννη Α. Αντωνιάδη για όλα αυτά τα χρόνια της συνεργασίας μας. Κοντά του γνώρισα ενδιαφέροντες κλάδους των μαθηματικών.

Πολλές ευχαριστίες χρωστώ στον καθηγητή Gerhard Frey (Duisburg-Essen, IEM) για την φιλοξενία που μου προσέφερε στο Ινστιτούτο Πειραματικών Μαθηματικών κατά τη διάρκεια της παραμονής μου στο Essen της Γερμανίας όπου και γράφτηκε ένα μέρος της εργασίας.

Με την ευκαιρία να ευχαριστήσω τον υποψήφιο διδάκτορα Roger Oyono που μοιραστήκαμε για τέσσερις μήνες το ίδιο γραφείο καθώς και τους υπόλοιπους φοιτητές του IEM τους οποίους γνώρισα.

Θα ήθελα να ευχαριστήσω επίσης τους καθηγητές Yves Edel (Heidelberg) και David Glynn (Canterbury, New Zealand) για την επικοινωνία που είχαμε και το υλικό που μου προσέφεραν. Η συνεισφορά τους ήταν ιδιαίτερα σημαντική για την κατανόηση εννοιών της Πεπερασμένης Γεωμετρίας και της σχέσης της με την Θεωρία Κωδικοποίησης.

Τέλος, ένα ευχαριστώ σε όλους τους φίλους μου που με βοήθησαν στην παρουσίαση της εργασίας.

Περιεχόμενα

Κεφάλαιο 3
Εύρεση και κατασκευή βέλτιστων κωδίκων δοσμένου μήκους

Κεφάλαιο 4
Αποκωδικοποίηση κωδίκων με τη χρήση βάσεων Gröbner

Κεφάλαιο 1

Βασικές έννοιες

1.1 Στοιχεία της Θεωρίας Κωδικοποίησης

Θα αναφερθούμε γενικά σε κάποια εισαγωγικά στοιχεία της Θεωρίας Κωδικοποίησης που θα μας είναι χρήσιμα στα κεφάλαια που ακολουθούν. Για περισσότερα στοιχεία παραπέμπουμε τον ενδιαφερόμενο αναγνώστη στο τρίτο κεφάλαιο του [Mag]. Οι αποδείξεις θεωρημάτων, προτάσεων κλπ, για τις οποίες δεν υπάρχει παραπομπή, υπάρχουν στο [Mag].

1.1.1 Ορολογία

Ένας $(n, M, d)_q$-κώδικας είναι ένα υποσύνολο του διανυσματικού χώρου $\mathbf{F}_q^n$, το οποίο αποτελείται από M διανύσματα με ελάχιστη απόσταση Hamming d. Ένας γραμμικός κώδικας είναι ένας διανυσματικός υπόχωρος του $\mathbf{F}_q^n$. Σε αυτή την περίπτωση το M είναι δύναμη του q.

Για ευκολία ένας γραμμικός $(n, q^k, d)_q$-κώδικας θα συμβολίζεται και ως $[n, k, d]_q$-κώδικας ή πιο απλά ως [n, k, d]-κώδικας, όταν είναι γνωστό σε ποιο σώμα αναφερόμαστε.

Θα αναφερόμαστε σε έναν $(n, M)_q$-κώδικα ή σε έναν $[n, k]_q$-κώδικα όταν δεν θέλουμε να αναφερθούμε στην ελάχιστη απόσταση του κώδικα.

Ορισμός 1.1.1.1 Απόσταση Hamming d(x, y) δύο διανυσμάτων x, y στο $\mathbf{F}_q^n$, με

$$x = x_1, x_2 \ldots, x_n \text{ και } y = y_1, y_2 \ldots, y_n,$$

είναι το πλήθος των συντεταγμένων στις οποίες τα x και y διαφέρουν. Δηλαδή

$$d(x, y) = \#\{i \in \mathbf{N}, 1 \le i \le n \mid x_i \ne y_i\}$$

Ορισμός 1.1.1.2 Βάρος (weight) Hamming w(x) ενός διανύσματος $x = x_1, x_2 \ldots, x_n$ στο $\mathbf{F}_q^n$ είναι το πλήθος των μη-μηδενικών συντεταγμένων του x. Δηλαδή,

$$w(x) = \#\{i \in \mathbf{N}, 1 \le i \le n \mid x_i \ne 0\}$$

Προφανώς, w(x) = d(x, 0).

Παρατήρηση 1.1.1.3 Η απόσταση Hamming είναι μια μετρική στον $\mathbf{F}_q^n$ και το βάρος Hamming w είναι μια νόρμα στον $\mathbf{F}_q^n$.

Ορισμός 1.1.1.4 Αν C είναι ένας $(n, k)_q$-κώδικας τότε **η ελάχιστη απόσταση d του κώδικα** είναι

$$d = \min_{\substack{u,v \in C \\ u \neq v}} d(u, v).$$

Πρόταση 1.1.1.5 Η ελάχιστη απόσταση ενός [n, k]-κώδικα είναι ίση με το ελάχιστο δυνατό βάρος που έχει κωδική λέξη διάφορη του μηδενικού στοιχείου.

Ορισμός 1.1.1.6 Ένας κώδικας ο οποίος **διορθώνει** το πολύ t λάθη θα λέγεται **t-κώδικας διόρθωσης λαθών** (**t-error-correcting code**), ενώ ένας κώδικας ο οποίος **ανιχνεύει** το πολύ e λάθη θα λέγεται **e-κώδικας ανίχνευσης λαθών** (**e-error-detecting code**).

Ορισμός 1.1.1.7 Ο **δυϊκός** (ή **ορθογώνιος) κώδικας** ενός $[n, k, d]_q$-κώδικα C ορίζεται να είναι

$$C^{\perp} = \{ x \mid u \cdot x = 0 \text{ για κάθε } u \in C\}$$

1.1.2 Φράγματα

Θεώρημα 1.1.2.1 (Φράγμα του Hamming) Οι παράμετροι ενός $(n. M)_q$-κώδικα ο οποίος διορθώνει t λάθη ικανοποιούν την ανισότητα

$$M\left(1 + (q-1)\binom{n}{1} + \ldots + (q-1)^t\binom{n}{t}\right) \leq q^n.$$

Αν όλα τα διανύσματα του $\mathbf{F}_q^n$ είναι μέσα σε σφαίρες κέντρου κωδικών λέξεων και ακτίνας t ενός $[n, k]_q$-κώδικα τότε παίρνουμε μια ειδική κατηγορία κωδίκων:

Ορισμός 1.1.2.2 Ένας t-κώδικας διόρθωσης λαθών ορισμένος στο σώμα $\mathbf{F}_q$ θα ονομάζεται **τέλειος** αν στο θεώρημα 1.1.2.1 ισχύει η ισότητα.

Αν ο C είναι κώδικας όπως αυτός του θεωρήματος 1.1.2.1 με ελάχιστη απόσταση d = 2t + 1, τότε αν διαγράψουμε από κάθε λέξη τα τελευταία d – 1 σύμβολα πάλι έχουμε έναν κώδικα με όλες τις κωδικές λέξεις διαφορετικές. Ο κώδικας που προκύπτει έχει μήκος n – d + 1, και παίρνουμε το

Θεώρημα 1.1.2.3 (Φράγμα του Singleton) Για έναν $[n. k, d]_q$-κώδικας ισχύει $|C| \leq q^{n-d+1}$. Δηλαδή $k \leq n - d + 1$.

Ορισμός 1.1.2.4 Ένας γραμμικός κώδικας θα λέγεται **διαχωρίσιμος μέγιστης απόστασης** (**maximum distance separable**) ή πιο απλά **κώδικας MDS** αν στο θεώρημα 1.1.2.3 ισχύει η ισότητα.

Συμβολισμός 1.1.2.5 Έστω C γραμμικός κώδικας. Θα συμβολίζουμε με G έναν **γεννήτορα πίνακα** (generator matrix) και με H έναν **πίνακα ελέγχου ισοτιμίας** (parity-check matrix) του C. Θα συμβολίζουμε με mld(H) τον ελάχιστο αριθμό των γραμμικά εξαρτημένων στηλών του H.

Παρατήρηση 1.1.2.6 Επειδή οποιεσδήποτε rank(H) + 1 το πλήθος στήλες του H είναι γραμμικά εξαρτημένες προφανώς ισχύει, mld(H) ≤ rank(H) + 1 για κάθε πίνακα H.

Θεώρημα 1.1.2.7 Για κάθε [n, k, d]-κώδικα (με n > k) ισχύουν:

(i) $k = n - \text{rank}(H)$
(ii) $d = \text{mld}(H)$
(iii) $d \le n - k + 1$.

Θεώρημα 1.1.2.8 (Φράγμα των Gilbert – Varshamov)

Αν

$$q^{n-k+1} > \sum_{i=0}^{d-1} \binom{n}{i} (q-1)^i$$

τότε μπορούμε να κατασκευάσουμε έναν $[n, k]_q$-κώδικα με ελάχιστη απόσταση μεγαλύτερη ή ίση από d.

Θεώρημα 1.1.2.9

Αν

$$q^{n-k} > \sum_{i=0}^{d-2} \binom{n-1}{i} (q-1)^i$$

τότε μπορούμε να κατασκευάσουμε έναν $[n, k, d]_q$-κώδικα. Επίσης, από κάθε $[n-1, k-1, d]_q$-κώδικα μπορούμε να κατασκευάσουμε έναν $[n, k, d]_q$-κώδικα.

Απόδειξη Χρήση του φράγματος των Gilber-Varshamov. Βλ. [Bie2], θεώρημα 13.2, σελίδα 79.

Παρατηρήστε ότι, το τελευταίο θεώρημα είναι ισχυρότερο του φράγματος των Gilbert-Varshamov. Βλ. [Bie2], λήμμα 13.1, σελίδα 80.

Θεώρημα 1.1.2.10 (Φράγμα του Plotkin) Ένας $[n, k, d]_q$-κώδικας ικανοποιεί την σχέση

$$d \le n \frac{q^k (q-1)}{(q^k - 1)q}.$$

Απόδειξη Βλ. [Lid], κεφάλαιο 4, θεώρημα 17.15, σελίδα 197.

Θεώρημα 1.1.2.11 (Φράγμα του Griesmer) Ένας $[n, k, d]_q$-κώδικας ικανοποιεί την σχέση

$$n \geq g_q(k, d) = \sum_{i=0}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil .$$

Απόδειξη Βλ. το [Gr] όπου βρίσκεται η απόδειξη ακριβώς όπως την έδωσε ο J.H. Griesmer, το 1960, για δυαδικούς κώδικες αλλά και το [S-S] όπου παρουσιάζεται η γενίκευση του φράγματος του Griesmer για όλους τους κώδικες.

1.2 Στοιχεία Πεπερασμένης Γεωμετρίας

Όπως θα φανεί σε επόμενα κεφάλαια η Θεωρία Κωδικοποίησης συνδέεται στενά με την Θεωρία της Πεπερασμένης Γεωμετρίας. Θα αναφερθούμε σε κάποια εισαγωγικά στοιχεία. Για κάποια επιπλέον στοιχεία παραπέμπουμε τον ενδιαφερόμενο αναγνώστη στο κεφάλαιο 2 του [Bie] αλλά και στο [Hil1].

1.2.1 Η προβολική γεωμετρία PG(r – 1, q)

Με τον διανυσματικό χώρο $\mathbf{F}_q^r = \{(\alpha_1, \alpha_2,\ldots, \alpha_r) \mid \alpha_i \in \mathbf{F}_q\}$, συνδέουμε μια συνδυαστική κατασκευή PG(r – 1, q) που αποτελείται από σημεία και ευθείες που ορίζονται ακολούθως.

- Τα *σημεία* του PG(r – 1, q) είναι οι μονοδιάστατοι υπόχωροι του $\mathbf{F}_q^r$.
- Οι *ευθείες* του PG(r – 1, q) είναι οι δισδιάστατοι υπόχωροι του $\mathbf{F}_q^r$.

Το σημείο P ανήκει στην ευθεία L αν και μόνο αν το P είναι υπόχωρος της L.

- Πιο γενικά ορίζουμε έναν **t-χώρο** (t-space) του PG(r – 1, q) να είναι ένας υπόχωρος του $\mathbf{F}_q^r$ διάστασης t + 1.

Επομένως, ο 0-χώρος είναι ένα σημείο και ο 1-χώρος μια ευθεία. Ένας 2-χώρος ονομάζεται **επίπεδο** (plane), ένας 3-χώρος ονομάζεται **στερεό** (solid) και ένας (r – 2)-χώρος στο PG(r – 1, q) ονομάζεται **υπερεπίπεδο** (hyperplane).

- Παρατηρήστε ότι η *διάσταση* t ενός t-χώρου στο PG(r – 1, q) είναι πάντα κατά ένα μικρότερη από την αντίστοιχη διάσταση του διανυσματικού χώρου.

Συνήθως, ταυτίζουμε έναν t-χώρο στο PG(r – 1, q) με το σύνολο των σημείων που περιέχει. Αφού ο (t + 1)-διανυσματικός υπόχωρος του $\mathbf{F}_q^r$ αποτελείται από $q^{t+1} - 1$ μη-μηδενικά διανύσματα και το καθένα έχει q – 1 μη-μηδενικά (βαθμωτά) πολλαπλάσια έχουμε ότι το πλήθος των σημείων ενός t-χώρου είναι $\frac{q^{t+1}-1}{q-1}$.

Το PG(r – 1, q) ονομάζεται η προβολική γεωμετρία των (r – 1)-διαστάσεων πάνω από το $\mathbf{F}_q$.

Κάθε σημείο P του PG(r – 1, q), σαν υπόχωρος του $\mathbf{F}_q^r$ μίας διάστασης, παράγεται από ένα μοναδικό μη-μηδενικό διάνυσμα. Επομένως αν $\mathbf{a} = (\alpha_1, \alpha_2,\ldots, \alpha_r) \in P$, τότε

$$P = \{\lambda\mathbf{a} \mid \lambda \in \mathbf{F}_q\}.$$

Στην πράξη, ταυτίζουμε το σημείο P με οποιοδήποτε μη-μηδενικό διάνυσμα περιέχεται σε αυτό. Με άλλα λόγια θεωρούμε τα σημεία του PG(r – 1, q) να είναι τα

μη-μηδενικά διανύσματα του $\mathbf{F}_q^r$ με τον κανόνα ότι αν $\mathbf{a} = (\alpha_1, \alpha_2, \ldots, \alpha_r)$ και $\mathbf{b} = (b_1, b_2, \ldots, b_r)$ είναι δύο τέτοια διανύσματα, τότε

$$\mathbf{a} = \mathbf{b} \text{ στο } PG(r-1, q) \text{ αν και μόνο αν } \mathbf{a} = \lambda\mathbf{b} \text{ στον } \mathbf{F}_q^r,$$

για κάποιο μη-μηδενικό λ στο $\mathbf{F}_q$.

Τώρα αναφέρουμε κάποιες στοιχειώδεις ιδιότητες του PG(r – 1, q).

Λήμμα 1.2.1.1 Στο PG(r – 1, q),

(i) το πλήθος των σημείων είναι $\frac{q^r - 1}{q - 1}$,

(ii) οποιαδήποτε δύο σημεία βρίσκονται πάνω σε ακριβώς μία ευθεία,

(iii) κάθε ευθεία περιέχει ακριβώς q + 1 σημεία,

(iv) κάθε σημείο βρίσκεται ακριβώς πάνω σε $\frac{q^{r-1} - 1}{q - 1}$ ευθείες.

(v) το πλήθος των (t + 1)-χώρων που περιέχουν έναν δοσμένο t-χώρο είναι $\frac{q^{(r-1)-t} - 1}{q - 1}$.

Απόδειξη

(i) Επειδή καθένα από τα $q^r - 1$ μη-μηδενικά διανύσματα του $\mathbf{F}_q^r$ έχει q – 1 μη-μηδενικά πολλαπλάσια, το πλήθος των σημείων του PG(r – 1, q) είναι $\frac{q^r - 1}{q - 1}$.

(ii) Αν τα **a** και **b** είναι διακριτά σημεία του PG(r – 1, q), τότε η μοναδική ευθεία μεταξύ τους αποτελείται από σημεία της μορφής λ**a** + μ**b** σημεία, όπου λ, μ $\in \mathbf{F}_q$ όχι και τα δύο μηδέν.

(iii) Στο (ii), υπάρχουν $q^2 - 1$ επιλογές για το ζευγάρι (λ, μ), αλλά επειδή ταυτίζουμε τα πολλαπλάσια, το πλήθος των διακριτών σημείων πάνω στην ευθεία είναι $\frac{q^2 - 1}{q - 1} = q + 1$.

(iv) Έστω t το πλήθος των ευθειών πάνω στις οποίες βρίσκεται ένα δοσμένο σημείο P. Έστω X το σύνολο

$$X = \{(Q, L) \text{ όπου Q είναι ένα σημείο διαφορετικό του P και L η ευθεία που συνδέει τα P και Q}\}.$$

Υπολογίζουμε τα στοιχεία του X με δύο τρόπους. Επειδή το PG(r – 1, q) έχει $\frac{q^r - 1}{q - 1}$ σημεία, έχουμε $\frac{q^r - 1}{q - 1} - 1$ επιλογές για το σημείο Q. Για καθεμία επιλογή για το Q υπάρχει μοναδική ευθεία L που ενώνει τα P και Q. Οπότε

$$|X| = \frac{q^r - 1}{q - 1} - 1 = \frac{q^r - q}{q - 1}.$$

Από την άλλη, για καθεμία από τις t ευθείες που διέρχονται από το P, υπάρχουν, από το (iii), q σημεία Q διαφορετικά από το P που βρίσκονται πάνω στην L. Οπότε

$$|X| = tq.$$

Εξισώνοντας τις δύο σχέσεις για το |X| παίρνουμε $\frac{q^r - q}{q - 1} = tq$. Οπότε,

$$t = \frac{q^{r-1} - 1}{q - 1}.$$

(v) Για ένα δοσμένο t-χώρο οι τρόποι που μπορούμε να επιλέξουμε ένα επιπλέον σημείο του PG(r – 1, q) για να παράγουμε έναν (t + 1)-χώρο είναι

$$\frac{q^r - 1}{q - 1} - \frac{q^{t+1} - 1}{q - 1} = \frac{q^r - q^{t+1}}{q - 1}.$$

Κάποια από αυτά τα επιπλέον σημεία παράγουν τον ίδιο (t + 1)-χώρο και επομένως πρέπει να διαιρέσουμε με

$$\frac{q^{t+2} - 1}{q - 1} - \frac{q^{t+1} - 1}{q - 1} = \frac{q^{t+2} - q^{t+1}}{q - 1},$$

το πλήθος των σημείων ενός τέτοιου (t + 1)-χώρου τα οποία δεν βρίσκονται στον δοσμένο t-χώρο.

Άρα έχουμε ότι στο PG(r – 1, q) το πλήθος των (t + 1)-χώρων που περιέχουν έναν δοσμένο t-χώρο είναι

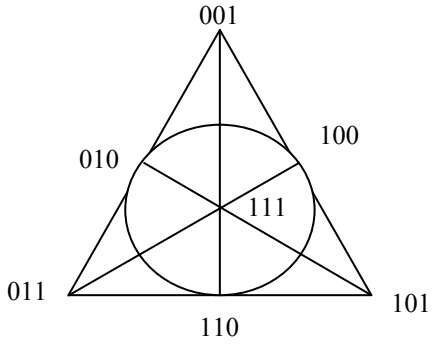
$$\frac{\frac{q^r - q^{t+1}}{q - 1}}{\frac{q^{t+2} - q^{t+1}}{q - 1}} = \frac{q^r - q^{t+1}}{q^{t+2} - q^{t+1}} = \frac{q^{t+1}\left(q^{(r-1)-t} - 1\right)}{q^{t+1}(q - 1)} = \frac{q^{(r-1)-t} - 1}{q - 1}.$$

Ορισμός 1.2.1.2 Την προβολική γεωμετρία PG(2, q) την ονομάζουμε **προβολικό επίπεδο** πάνω από το $\mathbf{F}_q$.

Παρατήρηση 1.2.1.3 Από το λήμμα 1.2.1.1 έπεται ότι η PG(2, q) είναι μια συμμετρική $(q^2 + q + 1, q + 1, 1)$-κατασκευή, άρα ο ορισμός που δώσαμε για το (πεπερασμένο) προβολικό επίπεδο συμφωνεί με τον ορισμό που δίνει ο Hill στο [Hil1]. (Βλ. τελική παρατήρηση 4(i), σελ. 26, [Hil1])

Παραδείγματα 1.2.1.4

(i) Το απλούστερο προβολικό επίπεδο είναι το PG(2, 2) το οποίο είναι γνωστό και σαν **το επίπεδο του Fano** (the Fano plane) προς τιμήν του Ιταλού μαθηματικού Gino Fano (1871-1952). Αποτελείται από 7 σημεία τα οποία ονομάζουμε 001, 010, 100, 011, 101, 110, 111 και 7 ευθείες όπως φαίνεται στο σχήμα 1. (Ο εγγεγραμμένος κύκλος του τριγώνου θεωρείται προβολικά ως ευθεία).



Σχήμα 1 – Το προβολικό επίπεδο PG(2, 2).

(ii) Τα 6 σημεία του PG(1, 5) είναι τα 01, 10, 11, 12, 13 και 14 και υπάρχει μια ακριβώς ευθεία που ενώνει τα 6 σημεία. Τα σημεία θα μπορούσαν ισοδύναμα να ονομαστούν, για παράδειγμα, και 03, 10, 22, 12, 21 και 41 αφού στο PG(1, 5) ισχύει 01 = 03, 11 = 22, 13 = 21 και 14 = 41.

Παρατηρήσεις 1.2.1.5

(1) Τα σημεία του PG(r – 1, q) μπορούν να οριστούν με μοναδικό τρόπο αν θέσουμε την αριστερότερη μη-μηδενική συντεταγμένη ίση με 1.
(2) Αν q = 2, τα σημεία του PG(r – 1, 2) αντιστοιχούνται στα μη-μηδενικά διανύσματα του $\mathbf{F}_2^r$.

Κεφάλαιο 2

Εύρεση και κατασκευή βέλτιστων γραμμικών κωδίκων δοσμένης ελάχιστης απόστασης

2.1 Εισαγωγή

Το **«κεντρικό πρόβλημα της θεωρίας κωδίκων»** είναι το πρόβλημα εύρεσης του $A_q(n, d)$, της μεγαλύτερης τιμής του M για την οποία υπάρχει $(n, M, d)_q$-κώδικας. Εμείς θα ασχοληθούμε με το ίδιο πρόβλημα, περιορισμένο στους γραμμικούς κώδικες. Αν q είναι δύναμη πρώτου, θα συμβολίζουμε με $B_q(n, d)$ την μεγαλύτερη τιμή του M, για την οποία υπάρχει *γραμμικός* $(n, M, d)_q$-κώδικας.
Προφανώς, το $B_q(n, d)$ είναι πάντοτε μια δύναμη του q, και $B_q(n, d) \leq A_q(n, d)$.

Θα αναφερόμαστε στο πρόβλημα εύρεσης του $B_q(n, d)$ ως το ***κεντρικό γραμμικό πρόβλημα της θεωρίας κωδίκων*** (the main linear coding theory problem) ή πιο σύντομα ως το MLCT πρόβλημα.

Αν θεωρήσουμε τις τιμές των q και d σταθερές, μπορούμε να διατυπώσουμε το πρόβλημα ως εξής.

Το MLCT-πρόβλημα (πρώτη εκδοχή) Για δοσμένο μήκος n, να βρεθεί η μέγιστη διάσταση k για την οποία υπάρχει ένας $[n, k, d]_q$-κώδικας.

Τότε, γι' αυτό το k, ισχύει $B_q(n, d) = q^k$.

Θυμίζουμε ότι το πλεόνασμα r ενός [n, k, d]-κώδικα είναι απλώς το n – k (το πλήθος των συμβόλων ελέγχου μιας κωδικής λέξης). Μια διαφορετική εκδοχή του MLCT-προβλήματος είναι:

Το MLCT-πρόβλημα (δεύτερη εκδοχή) Για δοσμένο πλεόνασμα r, να βρεθεί το μέγιστο μήκος n για το οποίο υπάρχει ένας $[n, n – r, d]_q$-κώδικας.

Η λύση της πρώτης εκδοχής για κάθε n είναι ισοδύναμη με τη λύση της δεύτερης εκδοχής για κάθε r, γιατί και στις δύο περιπτώσεις θα ξέρουμε ακριβώς αυτές τις τιμές των n και k για τις οποίες υπάρχει ένας [n, k, d]-κώδικας. Η ισοδυναμία των δύο εκδοχών θα δοθεί επακριβώς στο θεώρημα 2.1.7.

Αποδεικνύεται ότι η εκδοχή 2 εξασφαλίζει την πιο φυσική προσέγγιση. Η ιδέα αυτής της προσέγγισης, δίνεται στο επόμενο θεώρημα. Αλλά πρώτα ας δώσουμε κάποιους ορισμούς.

Ορισμός 2.1.1 Ένα (n, s)-σύνολο στο $\mathbf{F}_q^r$ είναι ένα σύνολο από n διανύσματα του $\mathbf{F}_q^r$ με την ιδιότητα οποιαδήποτε s από αυτά να είναι γραμμικά ανεξάρτητα.

Παρατήρηση 2.1.2 Προφανώς, όταν υπάρχει ένα (n, s)-σύνολο στο $\mathbf{F}_q^r$ υπάρχει και ένα (m, s)-σύνολο στο $\mathbf{F}_q^r$ για κάθε $m < n$ το οποίο προκύπτει από την αφαίρεση οποιονδήποτε (n – m) διανυσμάτων από το (n, s)-σύνολο.

Συμβολισμός 2.1.3 Συμβολίζουμε με $\max_s(r, q)$ τη μέγιστη τιμή του n για την οποία υπάρχει ένα (n, s)-σύνολο στο $\mathbf{F}_q^r$.

Ορισμός 2.1.4 Ένα (n, s)-σύνολο στο $\mathbf{F}_q^r$ για το οποίο ισχύει $n = \max_s(r, q)$ θα λέγεται **βέλτιστο (optimal)**.

Το packing πρόβλημα για το $\mathbf{F}_q^r$ είναι η εύρεση των διάφορων τιμών $\max_s(r, q)$ και των αντίστοιχων βέλτιστων (n, s)-συνόλων.

Το packing πρόβλημα πρώτη φορά μελετήθηκε από τον Bose (1947) για το στατιστικό του ενδιαφέρον και στη συνέχεια (1961) για την σύνδεσή του με την θεωρία κωδικοποίησης, η οποία δίνεται από το ακόλουθο θεώρημα.

Θεώρημα 2.1.5 Υπάρχει $[n, n – r, d]$-κώδικας στο $\mathbf{F}_q$ ακριβώς τότε όταν υπάρχει ένα (n, d – 1)-σύνολο του $\mathbf{F}_q^r$.

Απόδειξη Έστω C ένας $[n, n – r, d]_q$-κώδικας με πίνακα ελέγχου ισοτιμίας H. Ο H είναι ένας $r \times n$ πίνακας. Επειδή η ελάχιστη απόσταση του κώδικα είναι d έχουμε ότι οποιεσδήποτε d – 1 στήλες του H είναι γραμμικά ανεξάρτητες ενώ οποιεσδήποτε d στήλες του H είναι γραμμικά εξαρτημένες (βλ. και το θεώρημα 8.4 του [Hil1]). Άρα οι στήλες του H σχηματίζουν ένα (n, d – 1)-σύνολο στο $\mathbf{F}_q^r$.

Από την άλλη, έστω K ένα (n, d – 1)-σύνολο στο $\mathbf{F}_q^r$. Αν σχηματίσουμε έναν $r \times n$ πίνακα H με στήλες τα διανύσματα του K, τότε, (βλ. και το θεώρημα 8.4 του [Hil1]) ο H είναι ο πίνακας ελέγχου ισοτιμίας ενός $[n, n – r]$-κώδικα με ελάχιστη απόσταση το λιγότερο d.

Πόρισμα 2.1.6 Αν μας δοθούν τα q, d και r τότε η μεγαλύτερη τιμή για το n έτσι ώστε να υπάρχει ένας $[n, n – r, d]_q$-κώδικας είναι $\max_{d-1}(r, q)$.

Οπότε το MLCT πρόβλημα (εκδοχή 2) είναι το ίδιο με το packing πρόβλημα της εύρεσης του $\max_{d-1}(r, q)$. Στη συνέχεια δείχνουμε ότι οι τιμές του $B_q(n, d)$ δίνονται επίσης ως οι λύσεις αυτού του προβλήματος.

Θεώρημα 2.1.7 Έστω $\max_{d-1}(r – 1, q) < n \leq \max_{d-1}(r, q)$. Τότε, $B_q(n, d) = q^{n-r}$.

Απόδειξη Επειδή $n \leq \max_{d-1}(r, q)$ υπάρχει ένας $[n, n - r, d]_q$-κώδικας (πόρισμα 2.1.6) και επομένως $B_q(n, d) \geq q^{n-r}$. Αν το $B_q(n, d)$ ήταν γνήσια μεγαλύτερο από το q^{n-r} θα υπήρχε ένας $[n, n - r + 1, d]_q$-κώδικας που θα σήμαινε ότι $n \leq \max_{d-1}(r - 1, q)$, το οποίο είναι άτοπο λόγω της υπόθεσης.

Ας σκιαγραφήσουμε τι θα κάνουμε στις επόμενες παραγράφους του κεφαλαίου.

Θα ασχοληθούμε με το MLCT πρόβλημα για αυξανόμενες τιμές της ελάχιστης απόστασης d. Στην παράγραφο 2.2 θα ασχοληθούμε με τις περιπτώσεις $d = 1$ και $d = 2$ οι οποίες είναι εύκολες. Στην παράγραφο 2.3 θα θεωρήσουμε το πρόβλημα για $d = 3$ και θα το λύσουμε για όλες τις τιμές των q και r. Στη συνέχεια θα θεωρήσουμε την περίπτωση $d = 4$, θα τη λύσουμε για $q = 2$ και θα δώσουμε τα, μέχρι σήμερα, γνωστά αποτελέσματα για q μεγαλύτερο του 2. Για τις περιπτώσεις όπου το d είναι μεγαλύτερο του 4 πολύ λίγα πράγματα είναι γνωστά στη μορφή γενικών αποτελεσμάτων, τουλάχιστον μέχρι το d να φτάσει στην μέγιστη τιμή του για δεδομένο πλεόνασμα r, δηλαδή για $d = r + 1$.

2.2 Το MLCT πρόβλημα για d = 1 και d = 2

- Για d = 1. Επειδή ο ίδιος ο διανυσματικός χώρος $\mathbf{F}_q^n$ αποτελεί [n, n, 1]-γραμμικό κώδικα, έχουμε ότι $B_q(n, 1) = q^n$. Προφανώς ισχύει και $A_q(n ,1) = B_q(n, 1) = q^n$.

- Για d = 2. Θεωρούμε το γραμμικό κώδικα $C = \{x_1x_2 \dots x_n \mid x_1 + x_2 + \dots + x_n = 0\}$. Ο C είναι ένας [n, n – 1, 2]-κώδικας αφού το διάνυσμα 100...01 ανήκει στο C και δεν υπάρχει κωδική λέξη βάρους 1. Επειδή δεν υπάρχει γραμμικός [n, n, 2]-κώδικας έχουμε $B_q(n, 2) = q^{n-1}$.

2.3 Το MLCT πρόβλημα για d = 3 (ή αλλιώς οι κώδικες Hamming)

Θεώρημα 2.3.1 Για δοσμένο πλεόνασμα r, το μέγιστο μήκος n ενός $[n, n – r, 3]_q$-κώδικα είναι $\frac{q^r - 1}{q - 1}$ που σημαίνει ότι $\max_2(r, q) = \frac{q^r - 1}{q - 1}$.

Απόδειξη Από το πόρισμα 2.1.6 η απαιτούμενη τιμή του n για να υπάρχει ένας γραμμικός $[n, n – r, 3]_q$-κώδικας είναι $\max_2(r, q)$, το μεγαλύτερο μέγεθος ενός (n, 2)-συνόλου στο $\mathbf{F}_q^r$. Τώρα, ένα σύνολο S από διανύσματα στο $\mathbf{F}_q^r$ είναι ένα (n, 2)-σύνολο αν και μόνο αν δεν υπάρχει διάνυσμα στο S που να είναι (βαθμωτό) πολλαπλάσιο άλλου διανύσματος στο S. Όπως είναι γνωστό από την κατασκευή των κωδίκων Hamming πάνω από το $\mathbf{F}_q$ τα $q^r – 1$ μη μηδενικά διανύσματα στο $\mathbf{F}_q^r$ διαμερίζονται σε $\frac{q^r - 1}{q - 1}$ κλάσεις και κάθε κλάση περιέχει q – 1 διανύσματα για τα οποία το κάθε διάνυσμα είναι πολλαπλάσιο ενός άλλου διανύσματος της ίδιας κλάσης. Επομένως, ένα (n, 2)-σύνολο του μεγαλύτερου μεγέθους είναι απλά ένα σύνολο από $\frac{q^r - 1}{q - 1}$ διανύσματα που αποτελείται από ένα διάνυσμα από κάθε μια από αυτές τις κλάσεις.

Ο βέλτιστος [n, n – r, 3]-κώδικας με $n = \frac{q^r - 1}{q - 1}$ είναι ο κώδικας Hamming Ham(r, q).

Η λύση του MLCT προβλήματος (πρώτη εκδοχή) προκύπτει άμεσα από τα θεωρήματα 2.1.7 και 2.3.1.

Θεώρημα 2.3.2

$$B_q(n, 3) = q^{n-r}$$

όπου r είναι ο μοναδικός ακέραιος για τον οποίο ισχύει $\frac{q^{r-1} - 1}{q - 1} < n \le \frac{q^r - 1}{q - 1}$.

Παρατηρήσεις 2.3.3

(1) Είναι εύκολο να εκφραστεί το $B_q(n, 3)$ επακριβώς συναρτήσει των q και n. Συγκεκριμένα,

$$B_q(n, 3) = q^{[n-\log_q(nq-n+1)]}.$$

Απόδειξη Από το θεώρημα 2.3.1 υπάρχει $[n, n-r, 3]_q$-κώδικας αν και μόνο αν $n \leq \frac{q^r-1}{q-1}$.

Έχουμε ισοδύναμα:

$q^r \geq n(q-1)+1 \Leftrightarrow r \geq \log_q[n(q-1)+1] \Leftrightarrow n-r \leq n-\log_q[n(q-1)+1]$. Οπότε, πράγματι, $B_q(n, 3) = q^{[n-\log_q(nq-n+1)]}$.

(2) Για να κατασκευάσουμε έναν γραμμικό (n, M, 3)-κώδικα με $M = B_q(n, 3)$, βρίσκουμε τον μικρότερο ακέραιο r τέτοιο ώστε $n \leq \frac{q^r-1}{q-1}$ και τον γράφουμε σαν πίνακα ελέγχου ισοτιμίας, n διανύσματα-στήλες του $\mathbf{F}_q^r$ τέτοια ώστε καμία στήλη να είναι (βαθμωτό) πολλαπλάσιο κάποιας άλλης. Μπορούμε πάντα να πάρουμε έναν τέτοιο πίνακα ελέγχου-ισοτιμίας με το να διαγράψουμε στήλες από τον πίνακα ελέγχου-ισοτιμίας ενός κώδικα Hamming Ham(r, q). Επομένως, ο καλύτερος γραμμικός 1-διορθωτικός κώδικας δοσμένου μήκους είναι ή κάποιος πίνακας Hamming ή ένας shortened κώδικας Hamming.

- Πριν προχωρήσουμε στην περίπτωση όπου d = 4, παρατηρούμε ότι θα ήταν πλεονεκτικότερο να βλέπουμε ένα (n, s)-σύνολο όχι μόνο σαν ένα σύνολο διανυσμάτων του $\mathbf{F}_q^r$ αλλά και σαν ένα σύνολο σημείων της αντίστοιχης προβολικής γεωμετρίας PG(r – 1, q).

Ορισμός 2.3.4 Ένα σύνολο K που αποτελείται από n σημεία του PG(r – 1, q) ονομάζεται ένα (n, s)-σύνολο αν τα διανύσματα που αναπαριστούν τα σημεία του K σχηματίζουν ένα (n, s)-σύνολο στον αντίστοιχο (underlying) διανυσματικό χώρο $\mathbf{F}_q^r$.

Παρατηρήσεις 2.3.5

(1) Το να δουλεύουμε στο PG(r – 1, q) έχει δύο βασικά πλεονεκτήματα:
(a) κάποιοι σχετικά εύκολοι υπολογισμοί μπορούν να χρησιμοποιηθούν για να πάρουμε πάνω φράγματα του $\max_s(r, q)$ και
(b) πολλά βέλτιστα (n, s)-σύνολα είναι τελικά κάποιες φυσικές γεωμετρικές κατασκευές.

(2) Ένα (n, 2)-σύνολο του PG(r – 1, q) είναι απλά ένα σύνολο από n διακεκριμένα σημεία του PG(r – 1, q). Άρα μπορούμε να περιγράψουμε τον κώδικα Hamming Ham(r, q) ως τον κώδικα ο οποίος έχει πίνακα ελέγχου ισοτιμίας H τέτοιο ώστε

οι στήλες να είναι διακεκριμένα σημεία του PG(r – 1, q). Φυσικά, διαφορετικές αναπαραστάσεις αυτών των σημείων θα μας δίνουν διαφορετικούς, αλλά ισοδύναμους, κώδικες. Για παράδειγμα (βλ. το παράδειγμα 1.2.1.4(ii)) ο κώδικας Ham(1, 5) ορίζεται από τον πίνακα ελέγχου ισοτιμίας

$$H = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 2 & 3 & 4 \end{bmatrix}$$

ή ισοδύναμα

$$H = \begin{bmatrix} 0 & 1 & 2 & 1 & 2 & 4 \\ 3 & 0 & 2 & 2 & 1 & 1 \end{bmatrix}$$

2.4 Το MLCT πρόβλημα για d = 4

Εφαρμόζοντας το πόρισμα 2.1.6 για d = 4 προκύπτει ότι το μέγιστο μήκος ενός $[n, n - r, 4]_q$-κώδικα, για δοσμένο r, είναι ίσο με $max_3(r, q)$, το μεγαλύτερο μέγεθος ενός (n, 3)-συνόλου στο $\mathbf{F}_q^r$ (ή στο PG(r – 1, q)).

Θα εισάγουμε κάποια επιπλέον ορολογία η οποία θα μας φανεί χρήσιμη παρακάτω.

Ορισμός 2.4.1 Ένα (n, 3)-σύνολο στο επίπεδο PG(r – 1, q) (r ≥ 3) ονομάζεται **n-cap**. Αν r = 3, ένα (n, 3)-σύνολο στο επίπεδο PG(2, q) συνήθως ονομάζεται **n-τόξο** (n-arc).

Μπορούμε να γενικεύσουμε τον παραπάνω ορισμό για οποιοδήποτε (n, s)-σύνολο.

Ορισμός 2.4.2 Ένα (n, s)-σύνολο στο επίπεδο PG(r – 1, q) ονομάζεται (**n, s)-cap**.

Ορισμός 2.4.3 Ένα cap λέγεται **πλήρες** (complete) αν δεν περιέχεται σε κανένα cap του ίδιου προβολικού χώρου μεγαλύτερου μεγέθους.

Προφανώς, το μέγιστο πλήρες cap έχει μήκος ίσο με $max_3(r, q)$.

Επειδή τρία σημεία στο PG(r – 1, q) για r > 3 είναι γραμμικά εξαρτημένα αν και μόνο αν είναι συνευθειακά (δηλαδή βρίσκονται πάνω στην ίδια ευθεία) μπορούμε να περιγράψουμε ένα n-τόξο/n-cap σαν το σύνολο n σημείων όπου ανά τρία δεν είναι συνευθειακά.

Το πρόβλημα προσδιορισμού των τιμών του $max_3(r, q)$ πρώτα απασχόλησε τον Bose (1947). Λύθηκε γρήγορα για q = 2 και όλα τα r, καθώς και για r ≤ 4 και για όλα τα q. Αλλά, παρόλο που το πρόβλημα απέσπασε πολύ την προσοχή, λύθηκε επιπλέον μόνο για τα ζευγάρια (r, q) = (5, 3) και (6, 3). Το 1999, οι Yves Edel και Jürgen Bierbrauer με τη βοήθεια ηλεκτρονικών υπολογιστών έλυσαν το πρόβλημα για το ζευγάρι (5, 4). Οι γνωστές τιμές για το $max_3(r, q)$ εμφανίζονται στον παρακάτω πίνακα.

$max_3(r, 2) =$	2^{r-1}	(Bose 1947)
$max_3(3, q) =$	$q + 1$ αν q περιττός $q + 2$ αν q άρτιος	(Bose 1947)
$max_3(4, q) =$	$q^2 + 1$ αν q περιττός $q^2 + 1$ αν q άρτιος	(Bose 1947) (Qvist 1952)
$max_3(5, 3) =$	20	(Pellegrino 1970)
$max_3(6, 3) =$	56	(Hill 1973)
$max_3(5, 4) =$	41	(Edel, Bierbrauer 1999)

Πίνακας 2 – Οι γνωστές τιμές του $max_3(r, q)$

Στις επόμενες παραγράφους θα αποδείξουμε αυτά τα αποτελέσματα ή θα δώσουμε τα βασικά βήματα των αποδείξεων.

2.4.1 Ο προσδιορισμός του $\max_3 (r, 2)$

Ενδιαφερόμαστε για την εύρεση βέλτιστων *δυαδικών* γραμμικών κωδίκων με d = 4. Το ακόλουθο γενικό θεώρημα μας δείχνει ότι μπορούμε να αποκομίσουμε τέτοιους κώδικες από βέλτιστους κώδικες με ελάχιστη απόσταση 3 με την απλή σκέψη του να προσθέσουμε σε κάθε κωδική λέξη ένα σύμβολο ολικού ελέγχου ισοτιμίας.

Θεώρημα 2.4.1.1 Έστω d περιττός. Τότε υπάρχει δυαδικός [n, k, d]-κώδικας αν και μόνο αν υπάρχει δυαδικός [n + 1, k, d + 1]-κώδικας.

Απόδειξη Παρατηρήστε ότι ένας εκτεταμένος ("extended") γραμμικός κώδικας δηλαδή ο κώδικας που παίρνεται από έναν γραμμικό κώδικα με την προσθήκη σε κάθε κωδική λέξη ενός συμβόλου ολικού ελέγχου ισοτιμίας, είναι επίσης γραμμικός. Πιο συγκεκριμένα, αν το βάρος μια κωδικής λέξης είναι άρτιο προσθέτουμε ένα 0 ενώ αν το βάρος της είναι περιττό προσθέτουμε ένα 1. Αυτό αποδεικνύει την μια κατεύθυνση του θεωρήματος.

Για την αντίθετη κατεύθυνση, διαλέγουμε στον κώδικα [n + 1, k, d + 1] κωδικές λέξεις **x** και **y** τέτοιες ώστε $d(\mathbf{x}, \mathbf{y}) = d + 1$. Στη συνέχεια βρίσκουμε μια θέση στην οποία διαφέρουν και την διαγράφουμε από όλες τις κωδικές λέξεις. Το αποτέλεσμα είναι ένας [n, k, d]-κώδικας και αποδείξαμε το θεώρημα.

Από την απόδειξη φαίνεται ότι το θεώρημα γενικεύεται και για μη γραμμικούς κώδικες. Δηλαδή υπάρχει δυαδικός (n, M, d)-κώδικας αν και μόνο αν υπάρχει δυαδικός (n + 1, M, d + 1)-κώδικας. (Βλ. και θεώρημα 2.7 του [Hil1]).

Πόρισμα 2.4.1.2 Έστω d άρτιος. Τότε

(i) $B_2(n, d) = B_2(n - 1, d - 1)$
(ii) $\max_{d-1} (r, 2) = \max_{d-2} (r - 1, 2) + 1$.

Απόδειξη

(i) Άμεσο από το θεώρημα 2.4.1.1.
(ii) Έχουμε ισοδύναμα

$$\begin{aligned} & n \le \max_{d-1} (r, 2) \\ \Leftrightarrow\ & \text{υπάρχει δυαδικός } [n, n - r, d]\text{-κώδικας} \\ \Leftrightarrow\ & \text{υπάρχει δυαδικός } [n - 1, n - r, d - 1]\text{-κώδικας} \\ \Leftrightarrow\ & n - 1 \le \max_{d-1} (r - 1, 2) \\ \Leftrightarrow\ & n \le \max_{d-1} (r - 1, 2) + 1 \end{aligned}$$

Από όπου προκύπτει η ισότητα.

Πόρισμα 2.4.1.3 $\max_3 (r, 2) = 2^{r-1}$.

Απόδειξη

Από το θεώρημα 2.3.1 για q = 2 έχουμε ότι $\max_2(r, 2) = \frac{2^r - 1}{2 - 1} = 2^r - 1$. Οπότε, από το πόρισμα 1.11(ii), $\max_3(r, 2) = (2^{r-1} - 1) + 1 = 2^{r-1}$.

Ο βέλτιστος δυαδικός κώδικας με d = 4 και πλεόνασμα r είναι ο εκτεταμένος κώδικας Hamming $\hat{Ham}(r - 1, 2)$ (βλ. κεφάλαιο 8 του [Hil1]), ένας πίνακας ελέγχου ισοτιμίας για αυτόν τον κώδικα είναι

$$\hat{H} = \begin{bmatrix} & & & 0 \\ & H & & \vdots \\ & & & 0 \\ 1 & 1 & \ldots 1 & 1 \end{bmatrix},$$

όπου H είναι ένας πίνακας ελέγχου ισοτιμίας του κώδικα Ham(r – 1, 2) τέτοιος ώστε οι στήλες του H να είναι τα σημεία του PG(r – 2, 2) (για παράδειγμα τα μη-μηδενικά διανύσματα του $\mathbf{F}_2^{q-1}$.

Οι στήλες του $\hat{H}$ σχηματίζουν ένα βέλτιστο 2^{r-1}-cap στο PG(r – 1, 2) το οποίο αποτελείται από τα σημεία του PG(r – 1, 2) τα οποία <u>δεν</u> βρίσκονται στον υπόχωρο $\{(x_1, \ldots, x_r) \mid x_r = 0\}$. Γεωμετρικά, μπορεί να περιγραφεί σαν το συμπλήρωμα ενός υπερεπιπέδου.

2.4.2 Ο προσδιορισμός του $\max_3(3, q)$

Πρώτα θα δώσουμε κάποια παραδείγματα από καλούς γραμμικούς κώδικες με d = 4 και r = 3. Στη συνέχεια θα αποδείξουμε ότι αυτοί οι κώδικες είναι βέλτιστοι δείχνοντας ότι δεν υπάρχουν τέτοιοι κώδικες με μεγαλύτερο μήκος.

Θεώρημα 2.4.2.1 Έστω $a_1, a_2, \ldots, a_{q-1}$ τα μη-μηδενικά στοιχεία του $\mathbf{F}_q$.

(i) Ο πίνακας $H = \begin{bmatrix} 1 & 1 & \ldots & 1 & 1 & 0 \\ a_1 & a_2 & \ldots & a_{q-1} & 0 & 0 \\ a_1^2 & a_2^2 & \ldots & a_{q-1}^2 & 0 & 1 \end{bmatrix}$ είναι ο πίνακας ελέγχου ισοτιμίας ενός γραμμικού $[q + 1, q - 2, 4]$-κώδικα.

Ισοδύναμα, οι στήλες του H σχηματίζουν ένα (q + 1)-τόξο στο PG(2, q). Δηλαδή αποτελούν ένα (q + 1, 3)-σύνολο του PG(2, q).

(ii) Αν ο q είναι άρτιος τότε ο πίνακας

$$H^* = \begin{bmatrix} 1 & 1 & \ldots & 1 & 1 & 0 & 0 \\ a_1 & a_2 & \ldots & a_{q-1} & 0 & 1 & 0 \\ a_1^2 & a_2^2 & \ldots & a_{q-1}^2 & 0 & 0 & 1 \end{bmatrix}$$

είναι ο πίνακας ελέγχου ισοτιμίας ενός γραμμικού [q + 2, q – 1, 4]-κώδικα. Ισοδύναμα, οι στήλες του H^* σχηματίζουν ένα (q + 2)-τόξο στο PG(2, q). Δηλαδή αποτελούν ένα (q + 2, 3)-σύνολο του PG(2, q).

Απόδειξη

(i) Αρκεί να δείξουμε ότι, οποιεσδήποτε τρεις στήλες του H είναι γραμμικά ανεξάρτητες. Οποιεσδήποτε τρεις από τις πρώτες q – 1 στήλες του H σχηματίζουν έναν πίνακα Vandermonde. Είναι γνωστό ότι ένας πίνακας Vandermonde έχει μη-μηδενική ορίζουσα (θεώρημα 11.1 του [Hil1]) και ότι κάθε r × r πίνακας με μη-μηδενική ορίζουσα έχει r στήλες γραμμικά ανεξάρτητες (θεώρημα 11.2 του [Hil1]). Επομένως για οποιαδήποτε τριάδα στηλών, η οποία περιέχει μια ή δύο από τις δύο τελευταίες στήλες του H, η ορίζουσα μπορεί να αναπτυχθεί κατά μια από αυτές τις στήλες και να πάρουμε ξανά μια ορίζουσα ενός πίνακα Vandermonde. Πιο συγκεκριμένα, αν για παράδειγμα πάρουμε την ορίζουσα $\det\begin{bmatrix} 1 & 1 & 0 \\ a_i & a_j & 0 \\ a_i^2 & a_j^2 & 1 \end{bmatrix}$ μπορούμε να αναπτύξουμε ως προς την τελευταία στήλη οπότε θα πάρουμε $a_i - a_j$. Επειδή $a_i \neq a_j$ η ορίζουσα det A είναι μη-μηδενική.

(ii) Δείξαμε στο (i) ότι οποιεσδήποτε τρεις στήλες του H^* είναι γραμμικά ανεξάρτητες, με πιθανή εξαίρεση μια τριάδα της μορφής

$$\begin{bmatrix} 1 \\ a_i \\ a_i^2 \end{bmatrix}, \begin{bmatrix} 1 \\ a_j \\ a_j^2 \end{bmatrix} \text{ και } \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}.$$

Η ορίζουσα του πίνακα A που σχηματίζεται από αυτές τις τρεις στήλες είναι ίση με $a_i^2 - a_j^2$. Επειδή, το q είναι άρτιος, το σώμα $\mathbf{F}_q$ έχει χαρακτηριστική 2. Οπότε, $a_i^2 - a_j^2 = (a_i - a_j)^2$. Επομένως η ορίζουσα det A είναι μη-μηδενική αφού $a_i \neq a_j$.

Επειδή κατασκευάσαμε κώδικες μήκους q + 1 και q + 2 αντίστοιχα έχουμε το ακόλουθο

Πόρισμα 2.4.2.2 $\max_3 (3, q) \geq \begin{cases} q+1, & \text{αν q περιττός} \\ q+2, & \text{αν q άρτιος} \end{cases}$

Παρατήρηση 2.4.2.3 Το (q +1)-τόξο που σχηματίζεται από τις στήλες του H του θεωρήματος 2.4.2.1 είναι η κωνική τομή $\{(x, y, z) \in PG(2, q)$ όπου $yz = x^2\}$. Παρατηρήστε ότι τα στοιχεία της τρίτης γραμμής είναι ίσα με το γινόμενο των αντίστοιχων στοιχείων των δύο πρώτων γραμμών.

Τώρα θα δείξουμε ότι οι κώδικες/τόξα που δίνονται στο θεώρημα 2.4.2.1 είναι βέλτιστοι.

Θεώρημα 2.4.2.4

(i) Για κάθε δύναμη πρώτου q, $\max_3(3, q) \leq q + 2$.
(ii) Αν ο q είναι περιττός τότε $\max_3(3, q) \leq q + 1$.

Πρώτη απόδειξη

(i) Επειδή r = 3 είναι k = n – r = n – 3. Έστω H ο πίνακας ελέγχου ισοτιμίας, στην κανονική του μορφή, ενός γραμμικού $[n, n - 3, 4]_q$-κώδικα C με $n = \max_3 (3, q)$:

$$H = \begin{bmatrix} a_1 & a_2 & \ldots & a_{n-3} & 1 & 0 & 0 \\ b_1 & b_2 & \ldots & b_{n-3} & 0 & 1 & 0 \\ c_1 & c_2 & \ldots & c_{n-3} & 0 & 0 & 1 \end{bmatrix},$$

Επειδή d = 4 οποιεσδήποτε τρεις στήλες του H είναι γραμμικά ανεξάρτητες. Επομένως, η ορίζουσα που σχηματίζεται από οποιεσδήποτε τρεις στήλες του H είναι διαφορετική του μηδενός. Από το μη-μηδενισμό της ορίζουσας που σχηματίζεται από δυο από τις τρεις τελευταίες στήλες και από μια από τις n – 3 πρώτες, βρίσκουμε ότι όλα τα a_i, b_i, c_i είναι μη-μηδενικά. Πολλαπλασιάζοντας την i-στη στήλη με a_i^{-1} για i = 1, 2, …, n – 3 σχηματίζουμε έναν κώδικα ισοδύναμο με τον C όπου όλα τα a_i είναι όλα ίσα με 1. Επομένως, μπορούμε να υποθέσουμε ότι ο κώδικας ελέγχου ισοτιμίας είναι

$$H = \begin{bmatrix} 1 & 1 & \ldots & 1 & 1 & 0 & 0 \\ b_1 & b_2 & \ldots & b_{n-3} & 0 & 1 & 0 \\ c_1 & c_2 & \ldots & c_{n-3} & 0 & 0 & 1 \end{bmatrix},$$

όπου τα b_i και c_i είναι διαφορετικά του μηδενός. Επειδή η ορίζουσα που σχηματίζεται από την τελευταία στήλη και από δυο από τις n – 3 πρώτες στήλες, είναι μη-μηδενική, τα b_i πρέπει να είναι, σαν στοιχεία του $\mathbf{F}_q$, διαφορετικά ανά δύο. Επομένως, $n - 3 \leq q - 1$ οπότε $n \leq q + 2$.

(ii) (Προσαρμόστηκε από τους Fenton και Vámos, 1982). Ας υποθέσουμε ότι ο q είναι περιττός. Έστω ότι υπάρχει ένας γραμμικός $[q + 2, q - 1, 4]$-κώδικας. Θα καταλήξουμε σε άτοπο. Αν λοιπόν υπάρχει τέτοιος κώδικας, όπως και στο (i), μπορούμε να υποθέσουμε ότι ο C έχει πίνακα ελέγχου ισοτιμίας τον

$$H = \begin{bmatrix} 1 & 1 & \ldots & 1 & 1 & 0 & 0 \\ b_1 & b_2 & \ldots & b_{q-1} & 0 & 1 & 0 \\ c_1 & c_2 & \ldots & c_{q-1} & 0 & 0 & 1 \end{bmatrix}$$

όπου τα $b_1, b_2, \ldots, b_{q-1}$ είναι όλα τα μη-μηδενικά στοιχεία του $\mathbf{F}_q$ και τα $c_1, c_2, \ldots, c_{q-1}$ είναι όλα τα μη-μηδενικά στοιχεία του $\mathbf{F}_q$ σε κάποια σειρά. Ο μη-μηδενισμός των οριζουσών της μορφής

$$\det\begin{bmatrix} 1 & 1 & 1 \\ b_i & b_j & 0 \\ c_i & c_j & 0 \end{bmatrix}$$

μας δίνει ότι τα στοιχεία $b_1c_1^{-1}$, $b_2c_2^{-1}$, …, $b_{q-1}c_{q-1}^{-1}$ είναι όλα διαφορετικά μεταξύ τους ανά δύο άρα είναι επίσης τα μη-μηδενικά στοιχεία του $\mathbf{F}_q$ σε κάποια σειρά. Τώρα, επειδή κάθε στοιχείο του $\mathbf{F}_q$ έχει αντίστροφο διαφορετικό από τον εαυτό του εκτός από τα 1 και – 1 τα τρία γινόμενα $\prod_{i=1}^{q-1} b_i$, $\prod_{i=1}^{q-1} c_i$, $\prod_{i=1}^{q-1} b_i c_i^{-1}$ είναι όλα ίσα με – 1. Αλλά τότε

$$\prod_{i=1}^{q-1} b_i c_i^{-1} = (\prod_{i=1}^{q-1} b_i)(\prod_{i=1}^{q-1} c_i)^{-1} = (-1)(-1)^{-1} = 1.$$

Επειδή το q είναι περιττός $1 \neq -1$ και καταλήξαμε σε άτοπο.

Δεύτερη απόδειξη (γεωμετρική)

(i) Έστω K ένα n-τόξο στο PG(2, q) με μέγιστο μέγεθος $n = \max_3(3, q)$. Έστω P ένα σημείο του K. Από το λήμμα 1.2.1.1(iv) υπάρχουν q + 1 ευθείες που περνάνε από το P και κάθε σημείο του K βρίσκεται σε μια από αυτές τις ευθείες. Μάλιστα κάθε μια από αυτές τις ευθείες μπορεί να περιέχει, εκτός του P, ακριβώς ένα σημείο γιατί από τον ορισμό του n-τόξου δεν υπάρχουν τρία σημεία του K συνευθειακά (δηλαδή γραμμικά εξαρτημένα). Επομένως, $n \leq 1 + (q + 1) = q + 2$.

(ii) Έστω τώρα q περιττός. Έστω, με σκοπό να φτάσουμε σε άτοπο, ότι το K είναι ένα (q + 2)-τόξο στο PG(2, q). Δηλαδή το K περιέχει q + 2 σημεία τα οποία ανά τρία δεν είναι συνευθειακά. Αν P ένα τυχαίο σημείο του K, κάθε μια από τις q + 1 ευθείες που περνάνε από το P πρέπει να περιέχουν ακριβώς ένα επιπλέον σημείο από το K. Αυτό σημαίνει ότι κάθε ευθεία στο PG(2, q) τέμνει το K ή σε δύο σημεία ή σε κανένα, αλλά ποτέ σε ένα. Έστω, τώρα, Q ένα σημείο του PG(2, q) που δεν βρίσκεται στο K. Από το Q περνάνε q + 1 ευθείες και κάθε ένα σημείο του K βρίσκεται σε ακριβώς μια από αυτές. Άρα αν t από αυτές τις ευθείες τέμνουν το K σε δύο σημεία τότε |K| = 2t, άρτιος. Είναι άτοπο γιατί |K| = q + 2 περιττός.

Παρατήρηση 2.4.2.5 Η γεωμετρική απόδειξη είναι η καλύτερη από τις δύο αποδείξεις. Έχει δύο σημαντικά πλεονεκτήματα: (1) γενικεύεται για να δώσει άνω φράγματα στο $\max_3(r, q)$ για μεγαλύτερες τιμές του r και (2) δεν χρησιμοποιεί συγκεκριμένες ιδιότητες του σώματος $\mathbf{F}_q$ και επομένως δίνει κάποια άνω φράγματα για το μέγεθος των n-τόξων για οποιοδήποτε προβολικό επίπεδο με τάξη q.

Το πόρισμα 2.4.2.2 και το θεώρημα 2.4.2.4 μας δίνουν το

Θεώρημα 2.4.2.6 (Bose 1947 στο [Bos])

$$\max_3 (3, q) = \begin{cases} q + 1, & \text{αν q περιττός} \\ q + 2, & \text{αν q άρτιος} \end{cases}$$

Παρατήρηση 2.4.2.7 Ο Segre το 1954 (βλ. [Se1]) έδειξε ότι, για q περιττό, κάθε (q + 1)-τόξο στο PG(2, q) είναι μια κωνική τομή (conic). Από αυτό προκύπτει ότι ο βέλτιστος [q + 2, q – 1, 4]-κώδικας. είναι μοναδικός, μέχρι ισοδυναμίας. Για q άρτιο, τα βέλτιστα (q + 2)-τόξα στο PG(2, q) δεν είναι, εν γένει, μοναδικά και η κατάταξή τους είναι άγνωστη.

Ορισμός 2.4.2.8 Ένα (q+1)-cap στο PG(2, q) ονομάζεται **οβάλ** (oval) ενώ ένα (q+2)-cap στο PG(2, q) ονομάζεται **υπεροβάλ** (hyperoval).

Το θεώρημα 2.4.2.6 μας δείχνει ότι πάντα υπάρχει ένα oval στο PG(2, q) ενώ ένα υπεροβάλ υπάρχει στην περίπτωση όπου το q είναι περιττός.

2.4.3 Ο προσδιορισμός του $\max_3 (4, q)$, για q περιττό

Θα κάνουμε μια γεωμετρική προσέγγιση του προβλήματος. Αρχικά παρατηρούμε ότι ένας t-χώρος είναι απλά ένα αντίγραφο του PG(t, q) με την προϋπόθεση να λαμβάνονται υπ' όψιν και οι τυχόν ιδιότητες των υποχώρων του. Συγκεκριμένα, ένα cap στο PG(r – 1, q) πρέπει να τέμνει έναν (t – 1)-χώρο το πολύ σε $\max_3(t, q)$ σημεία, έχοντας πάντα υπ' όψιν ότι το υποσύνολο ενός cap είναι επίσης cap.

Τώρα θα παρουσιάσουμε ένα άνω φράγμα του $\max_3(4, q)$ όταν το q είναι περιττός.

Θεώρημα 2.4.3.1 Αν q περιττός τότε $\max_3(4, q) \leq q^2 + 1$.

Απόδειξη Ας υποθέσουμε ότι K είναι ένα n-cap στο PG(3, q) με μέγιστο μέγεθος. Δηλαδή ισχύει $n = \max_3(4, q)$. Θεωρούμε P_1 και P_2 δυο σημεία του K και L την ευθεία που ορίζουν τα P_1 και P_2. Επειδή δεν υπάρχουν τρία συνευθειακά σημεία στο K, η L δεν περιέχει άλλα σημεία του K. Σύμφωνα με το λήμμα 1.2.1.1(v) από την ευθεία L περνάνε q + 1 επίπεδα και κάθε σημείο του K, διαφορετικό από τα P_1 και P_2, βρίσκεται σε ακριβώς ένα από αυτά τα επίπεδα. Επειδή ο q είναι περιττός προκύπτει από το θεώρημα 2.4.2.4(ii) ότι κανένα επίπεδο δεν περιέχει πάνω από q + 1 σημεία του K. Συγκεκριμένα, ένα επίπεδο που τέμνει την ευθεία L μπορεί να περιέχει το πολύ q – 1 σημεία εκτός από τα P_1 και P_2. Οπότε

$$n \leq 2 + (q + 1)(q – 1) = q^2 + 1.$$

Στη συνέχεια δείχνουμε ότι υπάρχουν $(q^2 + 1)$-caps στο PG(3, q), όταν ο q είναι περιττός.

Θεώρημα 2.4.3.2 Υποθέτουμε q περιττός. Έστω b ένα στοιχείο του $\mathbf{F}_q$ όχι τετράγωνο. Τότε το σύνολο

$$Q = \{(x, y, z, w) \in PG(3, q) \text{ όπου } zw = x^2 - by^2\}$$

είναι ένα $(q^2 + 1)$-cap στο PG(3, q).

Απόδειξη Επειδή το b δεν είναι τετράγωνο το μόνο σημείο του Q με z = 0 είναι το (0, 0, 0, 1). Τα υπόλοιπα σημεία μπορούν να αναπαρασταθούν από ένα διάνυσμα με z = 1. Άρα μπορούμε να γράψουμε

$$Q = \{(0, 0, 0, 1), (x, y, 1, x^2 - by^2) \text{ όπου } x, y \in \mathbf{F}_q\} \quad (2.4.3.3)$$

Από εδώ φαίνεται ότι η τάξη του Q είναι $|Q| = q^2 + 1$. Πρέπει τώρα να δείξουμε ότι οποιαδήποτε τρία σημεία στο Q δεν είναι συνευθειακά. Προφανώς, το (0, 0, 0, 1) δεν είναι συνευθειακό με δύο άλλα σημεία του Q επειδή για κάθε δοσμένο ζευγάρι (x, y) υπάρχει μόνο ένα σημείο του Q της μορφής (x, y, 1, *). Έστω, λοιπόν $\mathbf{a}_1 = (x_1, y_1, 1, x_1^2 - by_1^2)$ και $\mathbf{a}_2 = (x_2, y_2, 1, x_2^2 - by_2^2)$ δύο σημεία του Q διαφορετικά από το (0, 0, 0, 1). Έστω, για να καταλήξουμε σε άτοπο, ότι η ευθεία που περνάει από τα $\mathbf{a}_1$ και $\mathbf{a}_2$ περιέχει και ένα τρίτο σημείο στο Q. Τότε, για κάποιο μη-μηδενικό λ ισχύει $\mathbf{a}_1 + \lambda\, \mathbf{a}_2 \in Q$. Δηλαδή, το σημείο

$$(x, y, z, w) = (x_1, y_1, 1, x_1^2 - by_1^2) + \lambda\,(x_2, y_2, 1, x_2^2 - by_2^2) =$$
$$(x_1 + \lambda x_2, y_1 + \lambda y_2, 1 + \lambda, x_1^2 - by_1^2 + \lambda x_2^2 - \lambda by_2^2)$$

ικανοποιεί την $zw = x^2 - by^2$. Αυτή η συνθήκη γράφεται

$$(1 + \lambda)(x_1^2 - by_1^2 + \lambda x_2^2 - \lambda by_2^2) = (x_1 + \lambda x_2)^2 - b(y_1 + \lambda y_2)^2 .$$

Ισοδύναμα,

$$x_1^2 - by_1^2 + \lambda x_2^2 - \lambda by_2^2 + \lambda x_1^2 - \lambda by_1^2 + \lambda^2 x_2^2 - \lambda^2 by_2^2 =$$
$$x_1^2 + 2\lambda x_1 x_2 + \lambda^2 x_2^2 - by_1^2 - 2\lambda by_1 y_2 - \lambda^2 by_2^2 .$$

Από όπου προκύπτει

$$\lambda x_1^2 + \lambda x_2^2 - \lambda by_1^2 - \lambda by_2^2 = 2\lambda x_1 x_2 - 2\lambda by_1 y_2.$$

Επειδή $\lambda \neq 0$ έπεται ότι

$$(x_1 - x_2)^2 = b(y_1 - y_2)^2,$$

το οποίο είναι άτοπο διότι το b δεν είναι τετράγωνο.

Τα θεωρήματα 2.4.3.1 και 2.4.3.2 μας δίνουν το

Θεώρημα 2.4.3.4 Αν q περιττός τότε $\max_3(4, q) = q^2 + 1$.

Παράδειγμα 2.4.3.5 Στο θεώρημα 2.4.3.2 θέτουμε q = 3 και b = – 1. Από την σχέση (2.4.3.3), ένα 10-cap στο PG(3, 3) παράγεται από τις στήλες του πίνακα

$$H = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 \\ 0 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 2 & 2 & 1 & 2 & 2 \end{bmatrix}.$$

Επομένως, ο Η είναι ο πίνακας ελέγχου ισοτιμίας του τριαδικού (ternary) γραμμικού [10, 6, 4]-κώδικα ο οποίος έχει μέγιστο μήκος για d = 4 και r = 4.

Διορθώνοντας τις στήλες του πίνακα ώστε το πρώτο μη-μηδενικό στοιχείο από πάνω προς τα κάτω να είναι 1 προκύπτει ο πίνακας:

$$\begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 2 & 0 & 2 & 1 \\ 0 & 1 & 1 & 2 & 1 & 1 & 1 & 2 & 2 & 2 \\ 1 & 0 & 1 & 2 & 1 & 2 & 2 & 2 & 1 & 1 \end{bmatrix}.$$

Παρατήρηση 2.4.3.6 Μπορεί να αποδειχθεί ότι ένα 10-cap στο PG(3, 3), όπως και ένα 4-cap στο PG(2, 3), είναι προβολικά μοναδικό.

2.4.4 Ο προσδιορισμός του max_3 (4, q), για q άρτιο

Θα παρουσιάσουμε ένα άνω φράγμα του $max_3(4, q)$ όταν το q είναι άρτιος.

Η απόδειξη ότι $max_3(4, 4) = 17$ δόθηκε από την Πολωνή Esther Seiden το 1950, η οποία, ωστόσο, δεν κατάφερε να γενικεύσει τις μεθόδους της για να δώσει περισσότερα αποτελέσματα.

Για να πάρουμε όλες τις τιμές του $max_3(4, q)$ για q άρτιο, θα ακολουθήσουμε μια διαδικασία ανάλογη με αυτήν που είδαμε στην περίπτωση που το q είναι περιττός. Αρχικά θα παρουσιάσουμε την μέθοδο του Bose για να πάρουμε ένα βέλτιστο άνω φράγμα και στη συνέχεια θα δώσουμε ένα cap που να ικανοποιεί την ισότητα.

Έστω Κ ένα cap στο PG(r – 1, q). Μια ευθεία ε του PG(r – 1, q) θα λέγεται **εφαπτόμενη** (tangent) του Κ αν έχει ακριβώς ένα κοινό σημείο με το Κ, αλλιώς, αν έχει δύο κοινά σημεία, θα λέγεται **τέμνουσα** (secant) του Κ. Αν η ευθεία ε δεν έχει κανένα κοινό σημείο με το Κ θα λέμε ότι η ε είναι **εξωτερική** (external) του Κ.

Θεώρημα 2.4.4.1 (Bose) Αν $q = 2^h$ $(h > 1)$ τότε $max_3(4, q) \leq q^2 + q + 2$.

Απόδειξη Ας υποθέσουμε ότι Κ είναι ένα n-cap στο PG(3, q). Θεωρούμε ένα σημείο Ρ του Κ. Από αυτό το σημείο περνάνε ακριβώς $\frac{q^3 - 1}{q - 1} = q^2 + q + 1$ ευθείες (βλ. λήμμα 1.2.1.1(iii)). Κάθε ευθεία περνάει από το πολύ ένα ακόμα σημείο μέσα στο Κ. Επομένως, το Κ περιέχει το πολύ $q^2 + q + 1 + 1 = q^2 + q + 2$ σημεία.

Θεώρημα 2.4.4.2 Αν $q = 2^h$ $(h > 1)$ τότε $\max_3(4, q) \leq q^2 + q + 1$.

Απόδειξη Υποθέτουμε ότι υπάρχει ένα n-cap, έστω K, στο PG(3, q) το οποίο έχει ακριβώς $q^2 + q + 2$ σημεία. Θα οδηγηθούμε σε άτοπο. Θεωρούμε ένα σημείο P του K. Κάθε μια από τις $q^2 + q + 1$ ευθείες του PG(3, q) που περνάνε από το P τέμνουν το K σε ακριβώς ένα επιπλέον σημείο. Διαφορετικά, το K θα είχε λιγότερα από $q^2 + q + 2$ σημεία. Επομένως, το K έχει μόνο τέμνουσες και δεν έχει εφαπτόμενες. Οπότε κάθε επίπεδο το οποίο τέμνει το K πρέπει να έχει τουλάχιστον $q + 2$ κοινά σημεία με το K, γιατί διαφορετικά θα μπορούσαμε να φέρουμε μια εφαπτόμενη στο K. Από την άλλη, κάθε επίπεδο είναι ένας 3-χώρος και επομένως έχει το πολύ $\max_3(3, q) = q + 2$ σημεία στο K (βλ θεώρημα 2.4.2.6). Επομένως, κάθε επίπεδο τέμνει το K ή σε ακριβώς $q + 2$ σημεία ή σε κανένα.

Επειδή μια ευθεία περνάει από ακριβώς δύο σημεία του K, το πλήθος των τεμνουσών του K είναι ίσο με το πλήθος των τρόπων που μπορούμε να επιλέξουμε δύο σημεία μέσα στο K, δηλαδή είναι ίσο με $\binom{q^2+q+2}{2} = \frac{1}{2}(q^2 + q + 2)(q^2 + q)$. Το πλήθος των ευθειών στο χώρο είναι $(q^2 + 1)(q^2 + q + 1)$. Επειδή $q > 1$ βλέπουμε ότι η δεύτερη ποσότητα είναι μεγαλύτερη από την πρώτη και επομένως υπάρχουν ευθείες του χώρου οι οποίες δεν τέμνουν το K.

Θεωρούμε L μια ευθεία η οποία δεν τέμνει το K. Θεωρούμε όλα τα επίπεδα που περιέχουν την L. Αυτά είναι σε πλήθος $q^2 + q + 1$. (βλ. λήμμα 1.2.1.1(v)). Κάθε ένα από αυτά τα επίπεδα, αν τέμνει το K, το τέμνει σε $q + 2$ σημεία. Έστω ότι t από αυτά τα επίπεδα τέμνουν το K. Τότε το K έχει $t (q + 2)$ σημεία. Δηλαδή, $q^2 + q + 2 = t (q + 2)$. Δηλαδή θα πρέπει

$$q^2 = (t - 1)(q+2)$$

όπου $q = 2^h$ $(h > 1)$ άρα και $t - 1 > 0$. Επομένως, το $q + 2$ διαιρεί το q^2 που σημαίνει ότι το 2 $(2^{h-1} + 1)$ διαιρεί το 2^{2h}. Δηλαδή το $2^{h-1} + 1$ (περιττός) διαιρεί το 2^{2h-1} (δύναμη του 2). Καταλήξαμε σε άτοπο άρα δεν υπάρχει cap με $q^2 + q + 2$ σημεία στο PG(3, q).

Θεώρημα 2.4.4.3 Αν $q = 2^h$ $(h > 1)$ τότε δεν υπάρχει n-cap στο PG(3, q) με $q^2 + 1 < n < q^2 + q + 2$.

Απόδειξη Ας υποθέσουμε ότι K είναι ένα n-cap στο PG(3, q) με $n = q^2 + \alpha$ όπου $1 < \alpha < q + 2$ και ότι δεν υπάρχει cap στο PG(3, q) με περισσότερα σημεία. Θα οδηγηθούμε σε άτοπο.

Θεωρούμε ένα σημείο P του K. Μπορούμε να συνδέσουμε το P με κάθε άλλο σημείο του K. Οπότε από το P περνάνε ακριβώς $q^2 + \alpha - 1$ τέμνουσες και υπάρχουν ακόμη $q^2 + q + 1 - (q^2 + \alpha - 1) = q + 2 - \alpha$ (> 0) ευθείες οι οποίες εφάπτονται του K στο σημείο P.

Έστω L μια εφαπτόμενη στο K στο σημείο P. Θεωρούμε τα $\frac{q^2-1}{q-1} = q + 1$ επίπεδα που περιέχουν την εφαπτόμενη L. Τα ονομάζουμε E_i όπου i = 1, 2, ..., q + 1. Κάθε $K \cap E_i$ είναι ένα (q + 1)-cap. Επειδή κανένα $K \cap E_i$ δεν μπορεί να έχει εφαπτόμενη (βλ. σελίδα 10 του [Qv]), τα E_i τέμνουν το K το πολύ σε q σημεία πέραν του P.

Αν υποθέσουμε ότι κάθε ένα από τα q + 1 επίπεδα τέμνει το K το πολύ σε q – 1 σημεία πέραν του P θα έχουμε ότι το K έχει συνολικά το πολύ $(q – 1)(q + 1) +1 = q^2$ σημεία. Το όποιο είναι άτοπο γιατί υποθέσαμε ότι το K έχει $q^2 + \alpha$ σημεία όπου $\alpha > 1$.

Επομένως, κάποια από τα q + 1 επίπεδα που περιέχουν την εφαπτόμενη L τέμνουν το K σε q σημεία. Χωρίς βλάβη της γενικότητας μπορούμε να υποθέσουμε ότι το E_1 τέμνει το K σε q + 1 σημεία.

Έχουμε ότι οι εφαπτόμενες του $K \cap E_1$ τέμνονται σε ένα σημείο εκτός του $K \cap E_1$ (βλ. θεώρημα 5 του [Qv]). Έστω Q αυτό το σημείο. Προφανώς το Q δεν ανήκει στο K. Οι εφαπτόμενες του $K \cap E_1$ είναι προφανώς και εφαπτόμενες του K.

Συνδέουμε το Q με όλα τα σημεία του K. Αν όλες οι ευθείες που συνδέουν το Q με το K ήταν εφαπτόμενες στο K θα προέκυπτε ένα νέο cap αποτελούμενο από όλα τα σημεία του K και το Q. Δηλαδή ένα cap με $q^2 + \alpha + 1$ σημεία. Το οποίο είναι άτοπο αφού έχουμε υποθέσει ότι δεν υπάρχει cap με περισσότερα σημεία από το K.

Έστω λοιπόν L_1 μια τέμνουσα του K που περνάει από το Q και τέμνει το K στα σημεία A και B. Η L_1 δεν ανήκει στο $K \cap E_1$ αφού το $K \cap E_1$ περιέχει μόνο εφαπτόμενες του K. Τα επίπεδα που περιέχουν την L_1 και τα οποία έχουν μια εφαπτόμενη με το $K \cap E_1$ είναι q + 1 στο πλήθος άρα είναι όλα τα επίπεδα που περιέχουν την L_1.

Άρα κάθε ένα από τα q + 1 επίπεδα τα οποίο περιέχει την L_1 έχει μια εφαπτόμενη με το K. Άρα περιέχει το πολύ q + 1 σημεία. (Στην γεωμετρική απόδειξη του θεωρήματος 2.4.2.4 δείξαμε ότι ένα (q+2)-τόξο έχει μόνο τέμνουσες και καθόλου εφαπτόμενες. Αυτό ήταν ανεξάρτητο του αν το q είναι άρτιος ή περιττός). Δηλαδή κάθε επίπεδο περιέχει το πολύ q – 1 σημεία εκτός των A και B. Συνολικά επομένως έχουμε ότι το K έχει το πολύ $(q + 1)(q – 1) + 2 = q^2 + 1$. Το όποιο είναι και πάλι άτοπο γιατί υποθέσαμε ότι το K έχει $q^2 + \alpha$ σημεία όπου $\alpha > 1$.

Δείξαμε δηλαδή ότι δεν υπάρχει $(q^2 + \alpha)$-cap στο PG(3, q) όπου $1 < \alpha < q + 2$. Αυτό ολοκληρώνει και την απόδειξη.

Παρατηρήστε ότι αν q = 2 τότε $\max_3(3, 2) = 8 \neq 2^2 + 1$. Άρα η εξαίρεση της περίπτωσης q = 2 ήταν απαραίτητη.

Τα θεωρήματα 2.4.4.1, 2.4.4.2 και 2.4.4.3 μας δίνουν το

Θεώρημα 2.4.4.4 (Qvist, 1952 στο [Qv]) Αν $q = 2^h$ $(h > 1)$ τότε $\max_3(4, q) \leq q^2 + 1$.

Στη συνέχεια δείχνουμε ότι υπάρχουν $(q^2 + 1)$-caps στο PG(3, q) όταν το q είναι άρτιος.

Αρχικά βρίσκουμε ένα στοιχείο b του $\mathbf{F}_q$ τέτοιο ώστε η εξίσωση

$$X^2 + Y^2 + bXY = 0 \qquad (1)$$

να έχει μοναδική λύση στο $\mathbf{F}_q \times \mathbf{F}_q$ την (x, y) = (0, 0). Παρατηρούμε ότι αν x = 0 τότε και y = 0 και αντίστροφα. Για να δείξουμε ότι υπάρχει τέτοιο b συμβολίζουμε το $\frac{X}{Y}$ με r και προσπαθούμε να επιλέξουμε τέτοιο b ώστε η εξίσωση

$$r^2 + br + 1 = 0 \qquad (2)$$

να μην έχει λύσεις στο $\mathbf{F}_q$.

Η τελευταία εξίσωση έχει το πολύ δύο λύσεις. Επίσης, αν r είναι μια λύση της (2) τότε και η r + b είναι λύση της αφού

$$(r + b)^2 + b\,(r + b) + 1 = r^2 + b^2 + br + b^2 + 1 = r^2 + br + 1 = 0.$$

Στην περίπτωση που b = 0 η εξίσωση έχει μοναδική λύση, την r = 1. Επίσης ισχυριζόμαστε ότι αν θεωρήσουμε διαφορετικές, μη-μηδενικές, τιμές του b δεν προκύπτει ίδια τιμή για το r. Πράγματι αν $b_1 \neq b_2$ τότε θεωρούμε τις εξισώσεις

$$r^2 + b_1 r + 1 = 0$$
$$r^2 + b_2 r + 1 = 0$$

Με αφαίρεση κατά μέλη των παραπάνω εξισώσεων προκύπτει ότι

$$(b_2 - b_1)\, r = 0$$

Οπότε, υποχρεωτικά, r = 0. Το οποίο είναι άτοπο, αφού η (2) δεν έχει το μηδέν σαν λύση.

Αν λοιπόν το r διατρέξει όλες τις τιμές του $\mathbf{F}_q$ για κάθε $r \neq 0$ υπάρχει μια τιμή για το b για την οποία το r να είναι λύση της εξίσωσης. Αν $r \neq 1$ τότε παίρνουμε ακριβώς ένα ζευγάρι διαφορετικών τιμών του b ενώ αν r = 1 παίρνουμε b = 0. Τέλος, αν r = 0 δεν παίρνουμε καμία τιμή του b. Οπότε,

$$\frac{1}{2}\,(q - 2) + 1 = \frac{1}{2}q - 1 + 1 = \frac{1}{2}q$$

τιμές του b μας δίνουν λύσεις της εξίσωσης (2) στο $\mathbf{F}_q$. Άρα υπάρχουν $q - \frac{1}{2}q = \frac{1}{2}q$ τιμές του b ώστε η εξίσωση (2) να μην έχει λύση. Αυτό αποδεικνύει και τον ισχυρισμό ότι υπάρχει κάποιο b τέτοιο ώστε η (1) να έχει μοναδική λύση την (x, y) = (0, 0).

Θεώρημα 2.4.4.5 Υποθέτουμε q άρτιος. Έστω b ένα στοιχείο τέτοιο ώστε η (1) να έχει μοναδική λύση την (x, y) = (0, 0). Τότε το σύνολο

$$Q = \{(x,y, z, w) \in PG(3, q) \text{ όπου } x^2 + y^2 + bxy + zw = 0\}$$

είναι ένα $(q^2 +1)$-cap στο PG(3, q).

Απόδειξη Το μόνο σημείο του Q με z = 0 είναι το (0, 0, 0, 1). Τα υπόλοιπα στοιχεία μπορούν να αναπαρασταθούν από ένα διάνυσμα με z = 1. Άρα μπορούμε να γράψουμε

$$Q = \{(0, 0, 0, 1), (x, y, 1, x^2 + y^2 + bxy) \text{ όπου } x, y \in \mathbf{F}_q\}$$

Από εδώ φαίνεται ότι η τάξη του Q είναι $|Q| = q^2 + 1$. Πρέπει τώρα να δείξουμε ότι οποιαδήποτε τρία σημεία στο Q δεν είναι συνευθειακά.

Αρχικά δείχνουμε ότι το (0, 0, 0, 1) δεν είναι συνευθειακό με δύο άλλα σημεία του Q. Πράγματι αν για κάποια μη-μηδενικά λ_1, λ_2 στο $\mathbf{F}_q$ και για κάποια διακεκριμένα $(x_1, y_1, 1, x_1^2 + y_1^2 + bx_1y_1), (x_2, y_2, 1, x_2^2 + y_2^2 + bx_2y_2)$ σημεία του Q ισχύει

$$(0, 0, 0, 1) = \lambda_1(x_1, y_1, 1, x_1^2 + y_1^2 + bx_1y_1) + \lambda_2(x_2, y_2, 1, x_2^2 + y_2^2 + bx_2y_2)$$

τότε θα πρέπει $\lambda_1 + \lambda_2 = 0$. Δηλαδή $\lambda_1 = \lambda_2$. Οπότε, θα πρέπει

$$(0, 0, 0, 1) = (\lambda_1(x_1 + x_2) , \lambda_1 (y_1 + y_2), 0 , \lambda_1 (x_1^2 + y_1^2 + bx_1y_1 + x_2^2 + y_2^2 + bx_2y_2)).$$

Δηλαδή, $x_1 = x_2$ και $y_1 = y_2$. Το οποίο είναι άτοπο.

Έστω, λοιπόν $\mathbf{a}_1 = (x_1, y_1, 1, x_1^2 + y_1^2 + bx_1y_1)$ και $\mathbf{a}_2 = (x_2, y_2, 1, x_2^2 + y_2^2 + bx_2y_2)$ δύο διακεκριμένα σημεία του Q διαφορετικά από το (0, 0, 0, 1). Έστω, για να καταλήξουμε σε άτοπο, ότι η ευθεία που περνάει από τα $\mathbf{a}_1$ και $\mathbf{a}_2$ περιέχει και ένα τρίτο σημείο στο Q. Τότε, για κάποιο μη-μηδενικό λ ισχύει $\mathbf{a}_1 + \lambda\, \mathbf{a}_2 \in Q$. Δηλαδή, το σημείο

$$(x, y, z, w) = (x_1, y_1, 1, x_1^2 + y_1^2 + bx_1y_1) + \lambda\, (x_2, y_2, 1, x_2^2 + y_2^2 + bx_2y_2) =$$
$$(x_1 + \lambda x_2, y_1 + \lambda y_2, 1 + \lambda, x_1^2 + y_1^2 + bx_1y_1 + \lambda x_2^2 + \lambda y_2^2 + \lambda bx_2y_2)$$

ικανοποιεί την $zw = x^2 + y^2 + bxy$. Αυτή η συνθήκη γράφεται

$$(1 + \lambda)(x_1^2 + y_1^2 + bx_1y_1 + \lambda x_2^2 + \lambda y_2^2 + \lambda bx_2y_2) =$$
$$(x_1 + \lambda x_2)^2 + (y_1 + \lambda y_2)^2 + b(x_1 + \lambda x_2)(y_1 + \lambda y_2).$$

Ισοδύναμα,

$$x_1^2 + y_1^2 + bx_1y_1 + \lambda x_2^2 + \lambda y_2^2 + \lambda bx_2y_2 + \lambda x_1^2 + \lambda y_1^2 + \lambda bx_1y_1 + \lambda^2 x_2^2 + \lambda^2 y_2^2 + \lambda^2 bx_2y_2 =$$
$$x_1^2 + \lambda^2 x_2^2 + y_1^2 + \lambda^2 y_2^2 + bx_1y_1 + \lambda bx_1y_2 + \lambda by_1x_2 + \lambda^2 bx_2y_2.$$

Από όπου προκύπτει

$$\lambda x_2^2 + \lambda y_2^2 + \lambda b x_2 y_2 + \lambda x_1^2 + \lambda y_1^2 + \lambda b x_1 y_1 = \lambda b x_1 y_2 + \lambda b y_1 x_2.$$

Επειδή $\lambda \neq 0$ έπεται ότι

$$(x_1^2 + x_2^2) + (y_1^2 + y_2^2) + b(x_2 y_2 + x_1 y_1 + x_1 y_2 + y_1 x_2) = 0$$

Η τελευταία σχέση γράφεται και

$$(x_1 + x_2)^2 + (y_1 + y_2)^2 + b(x_1 + x_2)(y_1 + y_2) = 0.$$

Λόγω της ιδιότητας που έχει το b θα πρέπει $x_1 = x_2$ και $y_1 = y_2$ το οποίο είναι άτοπο.

Τα θεωρήματα 2.4.4.4 και 2.4.4.5 μας δίνουν το

Θεώρημα 2.4.4.6 Αν $q = 2^h$ $(h > 1)$ τότε $\max_3(4, q) = q^2 + 1$.

Παρατήρηση 2.4.4.7 Το σύνολο Q του θεωρήματος 2.4.3.2 της προηγούμενης παραγράφου είναι ένα παράδειγμα ενός ελλειπτικού quadric (elliptic quadric). Αν ο q είναι περιττός κάθε ελλειπτικό quadric είναι ένα $(q^2 + 1)$-cap και αντίστροφα (Barlotti 1955) κάθε $(q^2 + 1)$-cap είναι ένα ελλειπτικό quadric. Αυτό σημαίνει ότι ο βέλτιστος $[q^2 + 1, q^2 – 3, 4]$-κώδικας είναι μοναδικός μέχρι ισοδυναμίας.

Παράδειγμα 2.4.4.8 Έστω $\mathbf{F}_4 = \{0, 1, \omega, \omega^2\}$. Χρησιμοποιώντας την κατασκευή από το θεώρημα 2.4.4.5 μπορούμε να πάρουμε το 17-cap του PG(3, 4) το οποίο είναι:

1	0	0	0	1	ω^2	1	ω^2	ω	1	ω^2	ω	ω^2	0	1	0	ω
0	1	0	0	1	ω	1	ω	1	ω	ω^2	0	1	ω^2	0	ω	ω^2
0	0	1	0	1	1	0	0	1	1	1	ω	ω	ω	ω^2	ω^2	ω^2
0	0	0	1	0	0	1	1	1	1	1	1	1	1	1	1	1

Ορισμός 2.4.4.9 (από τον Segre) Ένα $(q^2 + 1)$-cap στο PG(3, q) θα ονομάζεται **ovoid**.

Αναφέρουμε, χωρίς απόδειξη, το παρακάτω

Θεώρημα 2.4.4.10 Στο PG(3, q) υπάρχουν δύο γνωστοί τύποι ovoids

1. **(Barlotti [Barl], Panella [Pan])** Για q περιττό ή q = 4 ένα ovoid είναι ένα ελλειπτικό quadric (δηλαδή το σύνολο των ριζών μιας μη-ιδιάζουσας ελλειπτικής τετραγωνικής μορφής).

- Θυμίζουμε ότι μια ελλειπτική τετραγωνική μορφή είναι ένα πολυώνυμο της μορφής $Q(x_1, x_2, \ldots, x_n) = x_1x_2 + \ldots x_{n-3}x_{n-2} + p(x_{n-1}, x_n)$ όπου $p(x_{n-1}, x_n)$ είναι μια ανάγωγη τετραγωνική μορφή 2 μεταβλητών. Για τον ορισμό μιας τετραγωνικής μορφής βλ. ορισμό 2.1.10 του [Edg].

2. **(Tits, [Tit])** Για $q = 2^{2e+1}$, $e \geq 1$ υπάρχει ένα ovoid το οποίο δεν είναι ελλειπτικό quadric. Το ονομάζουμε **Tits ovoid** και είναι προβολικά ισόμορφο με το σύνολο

$$K = \{(0, 1, 0, 0), (1, z, x, y) \text{ όπου } z = xy + x^{\sigma+2} + y^{\sigma}, \sigma = 2^{e+1}, x, y \in \mathbf{F}_q\}.$$

2.4.5 Οι τιμές του $B_q(n, 4)$, για $n \leq q^2 + 1$

Με την χρήση του θεωρήματος 2.1.7 μπορούμε να μεταφράσουμε άμεσα τα αποτελέσματα που βρήκαμε για το $\max_3(r, q)$ για $r = 2$ και 3 (πόρισμα 2.4.2.2) σε αποτελέσματα για το $B_q(n, 4)$.

Θεώρημα 2.4.5.1

Αν q περιττός τότε

$$B_q(n, 4) = \begin{cases} q^{n-3} & \text{για } 4 \leq n \leq q + 1 \\ q^{n-4} & \text{για } q + 2 \leq n \leq q^2 + 1 \end{cases}$$

Αν q άρτιος τότε

$$B_q(n, 4) = \begin{cases} q^{n-3} & \text{για } 4 \leq n \leq q + 2 \\ q^{n-4} & \text{για } q + 3 \leq n \leq q^2 + 1 \end{cases}$$

2.4.6 Παρατηρήσεις για το $max_3(r, q)$ για $r \geq 5$

Για r = 3 και r = 4 το packing πρόβλημα για caps στο PG(r – 1, q) ήταν σχετικά εύκολο να λυθεί λόγω της ύπαρξης φυσικών γεωμετρικών σχηματισμών (κωνικές τομές στο PG(2, q) και ελλειπτικών quadrics στο PG(3, q)) οι οποίοι ήταν βέλτιστα caps. Αλλά στο PG(r – 1, q) για $r \geq 5$ τα μεγάλα caps δεν φαίνεται να προκύπτουν με τόσο φυσικό τρόπο και επομένως το packing πρόβλημα είναι πολύ πιο δύσκολο. Όπως φαίνεται και από τον πίνακα 2 οι μόνες γνωστές τιμές του $max_3(r, q)$ για $q \neq 2$ και $r \geq 5$ είναι οι $max_3(5, 3) = 20$, $max_3(6, 3) = 56$ και $max_3(5, 4) = 41$.

Είναι εύκολο να κατασκευάσουμε 20-caps στο PG(4, 3) αλλά δύσκολο να δείξουμε ότι το 20 είναι το μέγιστο δυνατό μέγεθος. Αντίθετα, είναι σχετικά δύσκολο να περιγράψουμε ένα 56-cap στο PG(5, 3) αλλά μια σύντομη απόδειξη του ότι το 56 είναι το μέγιστο δυνατό δόθηκε από τους Bruen και Hirschfeld (1978) και θα την παρουσιάσουμε παρακάτω.

Στις επόμενες τρεις παραγράφους, θα ασχοληθούμε με τις υπόλοιπες γνωστές τιμές για το $max_3(r, q)$. Στην παράγραφο 2.4.7 θα δώσουμε την κατασκευή ενός 20-cap στο PG(4, 3) και θα αναφερθούμε σε κάποια γνωστά θέματα που αφορούν στα 20-caps στο PG(4, 3). Στην παράγραφο 2.4.8 θα δώσουμε μια απόδειξη ότι $max_3(6, 3) = 56$ και θα σκιαγραφήσουμε τα βήματα της απόδειξης ότι υπάρχει μοναδικό 56-caps στο PG(5, 3). Στην παράγραφο 2.4.9 θα δώσουμε τα βασικά σημεία της απόδειξης ότι $max_3(5, 4) = 41$.

Στην συνέχεια, στις επόμενες τρεις παραγράφους θα ασχοληθούμε με τα μέχρι σήμερα σημαντικότερα γνωστά φράγματα που υπάρχουν στις περιπτώσεις που η τιμή του $max_3r(r, q)$ είναι άγνωστη. Στην παράγραφο 2.4.10 θα δώσουμε την απόδειξη ενός γενικού αναδρομικού άνω φράγματος, το οποίο μάλιστα δεν μπορεί να βελτιωθεί περισσότερο. Στην παράγραφο 2.4.11 θα διατυπώσουμε τα φράγματα που είναι γνωστά για το $max_3(r, 3)$ για r = 7 την μικρότερη τιμή του r για την οποία το $max_3(r, 3)$ είναι άγνωστο. Θα σκιαγραφήσουμε τις βασικότερες ιδέες που κρύβονται πίσω από τις αποδείξεις των συγκεκριμένων φραγμάτων. Τέλος, στην παράγραφο 2.4.12 θα δώσουμε έναν πίνακα με τα μέχρι στιγμής γνωστά κάτω φράγματα για το $max_3(r, q)$ για $5 \leq r \leq 12$ και $q \leq 9$.

2.4.7 Pellegrino caps

Απόδειξη ότι $\max_3(5, 3) \geq 20$.

Αν το σύνολο $\{\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_{10}\}$ είναι ένα 10-cap στο PG(3, 3) τότε το σύνολο $\{(\mathbf{x}_1, 0), (\mathbf{x}_2, 0), \ldots, (\mathbf{x}_{10}, 0), (\mathbf{x}_1, 1), (\mathbf{x}_2, 1), \ldots, (\mathbf{x}_{10}, 1)\}$ είναι ένα 20-cap στο PG(4, 3). Ένα 10-cap στο PG(3, 3) δίνεται στο παράδειγμα 2.4.3.5. Ένα 20-cap στο PG(4, 3) παράγεται από τις στήλες του πίνακα

$$\left[\begin{array}{cccccccccc|cccccccccc}
0 & 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 \\
0 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 \\
0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 0 & 1 & 1 & 1 & 2 & 2 & 1 & 2 & 2 & 1 & 0 & 1 & 1 & 1 & 2 & 2 & 1 & 2 & 2 \\
\hline
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1
\end{array}\right]$$

Αυτή είναι μια γενική μέθοδος κατασκευής ενός 2n-cap στο PG(r, q) από ένα γνωστό n-cap στο PG(r – 1, q) (doubling construction).

$\max_3(5, 3) = 20$

Ο Pellegrino το 1970 στο [Pe] έδειξε ότι το 20 είναι το μέγιστο δυνατό μέγεθος ενός cap στο PG(4, 3). Έδειξε επίσης ότι υπάρχουν δύο διαφορετικοί τύποι 20-caps στο PG(4, 3), τους οποίους ονόμασε Γ και Δ (βλ. θεώρημα 3.1 και 4.1 του [Hil4] αλλά και το [Pe]), ωστόσο δεν ταξινόμησε πλήρως τα 20-caps στο PG(4, 3). Αυτό το έκανε ο Hill το 1983 στο [Hil4] όπου απέδειξε ότι προβολικά υπάρχουν 9 διαφορετικά 20-caps στο PG(4, 3). Μάλιστα, ονόμασε αυτά τα caps $\Gamma_1, \Gamma_2, \ldots, \Gamma_8$ και Δ. Αυτός ο συμβολισμός χρησιμοποιείται και από τους περισσότερους γεωμέτρες. Τα $\Gamma_1, \ldots \Gamma_8$ ανήκουν όλα σε έναν κώνο ενώ το Δ σε ένα μη-ιδιάζων quadric.

Με τη χρήση υπολογιστή βρίσκουμε ότι τα 9 διαφορετικά Pellegrino caps στη μορφή πινάκων είναι τα εξής:

1	2
1 0 0 0 0 1 1 1 0 1 1 0 2 0 0 2 2 2 1 1	1 0 0 0 0 1 1 1 0 1 2 0 2 1 2 0 1 2 1 0
0 1 0 0 0 1 1 0 1 1 0 2 0 2 1 2 1 0 2 1	0 1 0 0 0 1 1 0 1 1 0 2 1 2 0 2 1 2 0 1
0 0 1 0 0 1 0 1 1 0 1 2 0 1 2 2 0 1 1 2	0 0 1 0 0 1 0 1 1 0 1 1 2 2 0 0 1 1 2 2
0 0 0 1 0 0 1 1 1 0 0 0 1 1 1 1 2 2 2 2	0 0 0 1 0 0 1 1 1 0 0 0 0 0 1 1 1 1 1 1
0 0 0 0 1 0 0 0 0 1 1 1 1 1 1 1 1 1 1 1	0 0 0 0 1 0 0 0 0 1 1 1 1 1 1 1 1 1 1 1

3	4
1 0 0 0 0 1 1 1 0 1 2 0 2 1 2 0 1 2 1 1	1 0 0 0 0 1 1 1 0 1 2 0 2 1 2 0 1 1 0 0
0 1 0 0 0 1 1 0 1 1 0 2 1 2 0 2 1 2 0 2	0 1 0 0 0 1 1 0 1 1 0 2 1 2 0 2 1 0 1 0
0 0 1 0 0 1 0 1 1 0 1 1 2 2 0 0 1 1 2 0	0 0 1 0 0 1 0 1 1 0 1 1 2 2 0 0 1 2 2 2
0 0 0 1 0 0 1 1 1 0 0 0 0 0 1 1 1 1 1 2	0 0 0 1 0 0 1 1 1 0 0 0 0 0 1 1 1 1 1 2
0 0 0 0 1 0 0 0 0 1 1 1 1 1 1 1 1 1 1 1	0 0 0 0 1 0 0 0 0 1 1 1 1 1 1 1 1 1 1 1

5	6
1 0 0 0 0 1 1 1 0 1 2 0 2 1 2 0 2 2 1 2	1 0 0 0 0 1 1 1 0 1 2 0 2 1 1 1 0 1 0 0
0 1 0 0 0 1 1 0 1 1 0 2 1 2 0 2 2 1 2 2	0 1 0 0 0 1 1 0 1 1 0 2 1 2 1 0 1 0 1 0
0 0 1 0 0 1 0 1 1 0 1 1 2 2 0 0 1 0 0 2	0 0 1 0 0 1 0 1 1 0 1 1 2 2 1 2 2 1 1 2
0 0 0 1 0 0 1 1 1 0 0 0 0 0 1 1 1 2 2 2	0 0 0 1 0 0 1 1 1 0 0 0 0 0 1 1 1 2 2 2
0 0 0 0 1 0 0 0 0 1 1 1 1 1 1 1 1 1 1 1	0 0 0 0 1 0 0 0 0 1 1 1 1 1 1 1 1 1 1 1

7	8
1 0 0 0 0 1 1 1 0 1 2 0 2 2 0 1 1 1 0 0	1 0 0 0 0 1 1 1 0 1 2 1 0 2 1 0 2 1 0 2
0 1 0 0 0 1 1 0 1 1 0 2 1 0 2 1 0 2 1 0	0 1 0 0 0 1 1 0 1 1 0 2 2 2 0 1 1 0 1 2
0 0 1 0 0 1 0 1 1 0 1 1 2 0 0 1 2 0 1 2	0 0 1 0 0 1 0 1 1 0 1 2 0 1 2 2 0 1 1 2
0 0 0 1 0 0 1 1 1 0 0 0 0 1 1 1 1 2 2 2	0 0 0 1 0 0 1 1 1 0 0 0 1 1 1 1 2 2 2 2
0 0 0 0 1 0 0 0 0 1 1 1 1 1 1 1 1 1 1 1	0 0 0 0 1 0 0 0 0 1 1 1 1 1 1 1 1 1 1 1

9
1 0 0 0 0 1 1 1 2 1 1 2 0 1 0 1 2 1 1 2
0 1 0 0 0 1 1 0 1 1 0 1 1 2 0 1 0 2 0 1
0 0 1 0 0 1 0 1 1 0 1 1 0 0 2 2 1 1 2 2
0 0 0 1 0 0 1 1 1 0 0 0 1 1 1 1 2 2 2 2
0 0 0 0 1 0 0 0 0 1 1 1 1 1 1 1 1 1 1 1

Οι κατανομές βαρών φαίνονται στον πίνακα 3. Δεν υπάρχουν διανύσματα με βάρος μεταξύ 1 και 9.

Τα caps 1 και 8 έχουν ίδια κατανομή βαρών άρα συμπεραίνουμε ότι πρόκειται για τα Δ και Γ_1 caps (βλ. λήμμα 4.4 του [Hil4]). Το cap 1 είναι το Δ (βλ. παράδειγμα 4.2 του [Hil4] .

Χρησιμοποιώντας τον πίνακα κατανομής των συν-βαρών (coweights) των 20-caps (βλ. ορισμό στο [Hil4] σελ. 434 και πίνακα 3 στο ίδιο σελ. 439) αντιστοιχούμε τα caps που βρήκαμε παραπάνω με τις ονομασίες που τους έδωσε ο Pellegrino.

Βάρη/cap	1 (Δ)	2 (Γ_6)	3 (Γ_4)	4 (Γ_5)	5 (Γ_7)	6 (Γ_3)	7 (Γ_8)	8 (Γ_1)	9 (Γ_2)
10		6	4	2	12	4			
11		6	12	16		18	18		40
12	150	96	92	90	60	78	96	150	60
13		42	40	44	120	48	36		
14		42	42	34		36	36		120
15	72	18	20	24		26	18	72	
16		6	10	8	30		18		
17		6		4					
18	20	20	22	20	20	20	20	20	20
19						2			
20									2

Πίνακας 3 – Οι κατανομές βαρών στα Pellegrino caps

2.4.8 Hill cap

Απόδειξη ότι $\max_3(5, 3) \leq 56$ (Bruen και Hirschfeld , 1978 στο [Bru]).

Κάνοντας χρήση του λήμματος 1.2.1.1(v) θα δείξουμε ότι το 56 είναι το μέγιστο δυνατό μέγεθος ενός cap στο PG(5, 3).

Εφαρμόζοντας το λήμμα 1.2.1.1(v) στο PG(5, 3) ισχύουν τα ακόλουθα

a) Μια δοσμένη ευθεία περιέχεται σε $\frac{3^{5-1}-1}{3-1} = \frac{80}{2} = 40$ το πλήθος επίπεδα.

b) Ένα δοσμένο επίπεδο περιέχεται σε $\frac{3^{5-2}-1}{3-1} = \frac{26}{2} = 13$ το πλήθος στερεά

c) Ένα δοσμένο στερεό περιέχεται σε $\frac{3^{5-3}-1}{3-1} = \frac{8}{2} = 4$ το πλήθος 4-χώρους.

Ας υποθέσουμε, λοιπόν, ότι K είναι ένα cap στο PG(5, 3). Θα δείξουμε ότι το K έχει το πολύ 56 σημεία.

Αν όλα τα επίπεδα του PG(5, 3) τέμνουν το K το πολύ σε τρία σημεία τότε σε ένα δοσμένο επίπεδο κάθε ευθεία τέμνει το K το πολύ σε δύο σημεία και έχουμε το πολύ ένα ακόμα σημείο τομής του K με το επίπεδο. Επειδή κάθε ευθεία περιέχεται σε 40 επίπεδα έχουμε ότι $|K| \leq 40 + 2 = 42$. (Δύο σημεία σε μια δοσμένη ευθεία και το πολύ ένα ακόμα σημείο σε καθένα από τα 40 επίπεδα που την περιέχουν).

Ας υποθέσουμε λοιπόν ότι κάποιο επίπεδο π του PG(5, 3) τέμνει το K σε 4 σημεία. Ανάλογα, μπορούμε να υποθέσουμε ότι κάθε στερεό περιέχει το λιγότερο 8 σημεία του K. Γιατί διαφορετικά $|K| \leq 4 + 3 \cdot 13 = 43$. (4 σημεία στο π και το πολύ 3 σημεία σε καθένα από τα 13 στερεά που το περιέχουν). Τελικά, επειδή $\max_3(5, 3) = 20$, έχουμε $|K| \leq 8 + 4(20 - 8) = 56$.

Ένα 56-cap στο PG(5, 3)

Ο Hill το 1973 στο [Hil2] κατασκεύασε ένα 56-cap υποθέτοντας συγκεκριμένες μεταθετικές ιδιότητες της ομάδας αυτομορφισμών του. Το 56-cap είναι το ακόλουθο:

2000022 2021211 1000110 1211220 1001100 1001010 2111202
1200021 0220002 1100121 1002012 1101210 1101111 1022022
0120021 1010211 2110122 0011121 1111221 2111121 1210101
0012021 0122202 0211122 2212002 2112222 2212122 0202212
0001221 1000101 0021222 0102120 0212022 0222222 1101120
0000111 0121221 0002202 1221102 0022002 0020202 2221011

Είναι εύκολο να αποδειχθεί, με την χρήση της MAPLE, ότι οι στήλες του παραπάνω πίνακα είναι ανά τρεις γραμμικά ανεξάρτητες πάνω από το $\mathbf{F}_3$. Στην διεύθυνση http://www.math.uoc.gr/~marios/master/ μπορείτε να βρείτε ένα πρόγραμμα σε MAPLE το οποίο κάνει αυτό τον έλεγχο. (Το πρόγραμμα χρειάστηκε σε Pentium 4

με 2.6 GHz περίπου 15 λεπτά για να ολοκληρώσει τον έλεγχο). Άρα πράγματι, οι στήλες του αποτελούν ένα 56-cap στο PG(5, 3).

Μοναδικότητα του 56-cap στο PG(5, 3)

Ο Hill το 1978 απέδειξε ότι το 56-cap στο PG(5, 3) είναι προβολικά μοναδικό (Βλ. θεώρημα 8.1 του [Hil3]). Απέδειξε δηλαδή την μοναδικότητα ενός βέλτιστου $[56, 50, 4]_3$-κώδικα.).

Η απόδειξη της μοναδικότητας έγινε σε τρία βήματα:

Βήμα 1: Ο κώδικας C ενός 56-cap στο PG(5, 3) έχει μοναδική κατανομή βαρών, όπως επίσης μοναδική κατανομή βαρών έχει και ο κατάλοιπος κώδικας[1] C_1 του C.

Βήμα 2: Ένας κώδικας με την απαραίτητη κατανομή βαρών του C_1 υπάρχει και είναι μοναδικός.

Βήμα 3: Μια επέκταση του κώδικα C_1 σε cap-κώδικα με την απαραίτητη κατανομή βαρών υπάρχει και είναι μοναδική.

Η απόδειξη του πρώτου βήματος έγινε με την παρατήρηση ότι ο κώδικας C είναι **κώδικας 2 βαρών**, δηλαδή υπάρχουν δύο μη-μηδενικές κωδικές λέξεις με βάρη w_1, w_2 ($w_1 > w_2$) και κάθε μη-μηδενική κωδική λέξη έχει βάρος w_1 ή w_2. Συγκεκριμένα έδειξε ότι

Λήμμα 2.4.8.1

(i) Ο κώδικας C ενός 56-cap στο PG(5, 3) είναι ένας [56, 6]-κώδικας 2 βαρών με βάρη 45 και 36, πολλαπλότητας 56 και 308 αντίστοιχα.
(ii) Ο κατάλοιπος κώδικας C_1 του C είναι ένας [55, 5]-κώδικας 2 βαρών με βάρη 45 και 36, πολλαπλότητας 11 και 110 αντίστοιχα.

(Βλ. λήμμα 8.15 του [Hil3]).

Με όρους της πεπερασμένης γεωμετρίας θα λέγαμε ότι ο Hill έδειξε ότι το 56-cap στο PG(5, 3) τέμνει πάντοτε ένα υπερεπίπεδο σε 11 ή 20 σημεία.

Στη συνέχεια απέδειξε ότι

Πρόταση 2.4.8.2 Ένας προβολικός κώδικας 2 βαρών καθορίζεται μοναδικά από την κατανομή βαρών του, αν και μόνο αν ο δυαδικός του κώδικας καθορίζεται μοναδικά από την κατανομή βαρών του (βλ. πρόταση 8.9 του [Hil3]).

Η απόδειξη του δεύτερου βήματος (λήμμα 8.16 του [Hil3]) έγινε με την απλή παρατήρηση ότι ο $C_1^{\perp}$ είναι ένας [11, 5, 6]-κώδικας. Πιο συγκεκριμένα είναι ένας κώδικας 2 βαρών με βάρη 9 και 6, πολλαπλότητας 55 και 66 αντίστοιχα. Ο $C_1^{\perp}$ είναι ο πολύ γνωστός κώδικας Golay (βλ. παράδειγμα 8.11 του [Hil3]). Ένας τέτοιος κώδικας υπάρχει και είναι μοναδικός (βλ. θεώρημα 8.14 του [Hil3]).

[1] Για τον ορισμό του κατάλοιπου κώδικα βλ. τον ορισμό 3.3.1.8 στο επόμενο κεφάλαιο

Η απόδειξη της ύπαρξης και της μοναδικότητας του C_1 προκύπτει άμεσα από τη πρόταση 2.4.8.2.

Η απόδειξη του τρίτου βήματος στηρίζεται κατά κύριο λόγο στο παρακάτω

Λήμμα 2.4.8.3 Έστω C ένας $[56, 6]_3$-cap-κώδικας. Έστω d_1 και d_2 κωδικές λέξεις του C βάρους 45 και 35 αντίστοιχα. Έστω d μια οποιαδήποτε άλλη κωδική λέξη του C. Τότε

i) το d_1 και το d έχουν 2 ή 5 κοινά μηδενικά και
ii) το d_2 και το d έχουν 5 ή 8 κοινά μηδενικά

(βλ. λήμμα 2.4.8.3 του [Hil3]).

2.4.9 Ο προσδιορισμός του $max_3(5, 4)$

Στο [Ta] ο G. Tallini έδωσε το 1964 ένα κάτω φράγμα για το πλήθος των σημείων που μπορεί να έχει ένα πλήρες cap στο PG(4, q). Από αυτό το φράγμα προκύπτει ότι $max_3(5, 4) \geq 41$. Η απόδειξη του Tallini ωστόσο δεν είναι κατασκευαστική με αποτέλεσμα να μην δίνονται 41-caps στο PG(4, 4).

Σε αυτήν την παράγραφο θα συμβολίζουμε με A_i το πλήθος των κωδικών λέξεων βάρους i.

Απόδειξη ότι $max_3(5, 4) \leq 41$ (Edel και Bierbrauer, 1999 στο [BE])

Θα παρουσιάσουμε συνοπτικά την απόδειξη των Yves Edel και Jürgen Bierbrauer ότι δεν υπάρχουν 42-caps στο PG(4, 4) και επομένως ότι $max_3(5, 4) = 41$.

Η απόδειξη έχει ως εξής:

Έστω υπάρχει κάποιο 42-cap, έστω K, στο PG(4, 4). Θα συμβολίζουμε με α(i) το πλήθος των υπερεπιπέδων που τέμνουν το K σε ακριβώς i σημεία. Έστω $K = \{P_1, P_2, \ldots, P_{42}\}$.

Κατασκευάζουμε τον αντίστοιχο (42×5)-πίνακα $G = [P_1, P_2, \ldots, P_{42}]$ πάνω από το σώμα $\mathbf{F}_4$. Ο G είναι ο γεννήτορας πίνακας ενός $[42, 5]_4$-κώδικα C. Θα συμβολίζουμε τις γραμμές του G με γ_i, i = 1, 2, 3, 4, 5.

Έστω $x = (x_1, x_2, \ldots, x_{42})$ μια μη-μηδενική κωδική λέξη του C. Τότε $x = \sum_{i=1}^{5} \lambda_i \gamma_i$,

όπου $\lambda_i \in \mathbf{F}_4$.

Αν θεωρήσουμε το υπερεπίπεδο $H = (\lambda_1, \ldots, \lambda_5)^{\perp}$, ισχύει ότι $P_j \in H$ αν και μόνο αν $x_j = 0$. Οπότε υπάρχει μια 1-1 αντιστοιχία μεταξύ των υπερπεπιπέδων που τέμνουν το K σε i σημεία και των 1-διάστατων υπόχωρων του κώδικα C των οποίων τα μη-μηδενικά διανύσματα έχουν βάρος 42 – i. (Βλ. επίσης [BE] αλλά και [BP] παράγραφος 1.3.4 σελίδα 11).

Αυτό αποδεικνύει ότι

$$A_i = 3 \cdot \alpha(42 - i) \qquad (2.4.9.1)$$

Ένα πρώτο στοιχείο που προκύπτει άμεσα από τον τελευταίο τύπο είναι ότι

Λήμμα 2.4.9.2 Οι κωδικές λέξεις του κώδικα C είναι πολλαπλάσια του 3.

Στη συνέχεια βρίσκουμε την μέγιστη δυνατή ελάχιστη απόσταση ενός $[42, 5]_4$-κώδικα, ώστε να προσδιορίσουμε τον μέγιστο αριθμό σημείων που τέμνει ένα υπερπεπίπεδο το K.

Αυτό γίνεται ως εξής:

Θα δείξουμε στο κεφάλαιο 3 ότι δεν υπάρχει $[10, 3, 7]_4$-κώδικας. Άρα, αν θεωρήσουμε έναν $[10, 3]_4$-κώδικα.με μέγιστη ελάχιστη απόσταση, αυτή είναι το πολύ 6. Στη συνέχεια με truncation παίρνουμε ένα $[11, 3]_4$-κώδικα με ελάχιστη απόσταση το πολύ 7. Με shortening παίρνουμε ένα $[12, 4]_4$-κώδικα με ελάχιστη απόσταση το πολύ 7. Έχοντας αυτό ως δεδομένο, αν εφαρμόσουμε το φράγμα του Griesmer για $[42, 5]_4$-κώδικες, βλέπουμε ότι η μέγιστη δυνατή ελάχιστη απόσταση είναι το πολύ 29.

Ας βρούμε τώρα και ένα κάτω φράγμα. Στο [Liz] αποδεικνύεται, με κατασκευή, ότι η μέγιστη ελάχιστη απόσταση ενός $[43, 5]_4$-κώδικα είναι το μεγαλύτερη ίση από 30. Με truncation έχουμε ότι για $[42, 5]_4$-κώδικες η μέγιστη δυνατή ελάχιστη απόσταση είναι το λιγότερο 29.

Συνδυάζοντας τα παραπάνω βλέπουμε ότι, η μέγιστη δυνατή ελάχιστη απόσταση ενός $[42, 5]_4$-κώδικα είναι 29. (Βλ. και [Br]).

Οπότε ένα υπερεπίπεδο Η τέμνει το Κ το λιγότερο σε 42 – 29 = 13 σημεία.

Λήμμα 2.4.9.2 Αν υπάρχει κάποιο 42-cap, έστω Κ, στο PG(4, 4) τότε υποχρεωτικά υπάρχει ένα υπερπεπίπεδο Η το οποίο τέμνει το Κ το λιγότερο σε 13 σημεία.

Το $K \cap H$ είναι και αυτό cap στο PG(3, 4). Το $\max_3(3, q)$ για $q = 4$ είναι $4^2 + 1 = 17$. Άρα το $K \cap H$ έχει το πολύ 17 σημεία.

Από το λήμμα 2.4.9.2 και την τελευταία παρατήρηση προκύπτει το παρακάτω

Λήμμα 2.4.9.3 Αν υπάρχει κάποιο 42-cap, έστω Κ, στο PG(4, 4) τότε υποχρεωτικά υπάρχει ένα υπερπεπίπεδο Η τέτοιο ώστε $13 \leq | K \cap H | \leq 17$.

Στη συνέχεια αυτή η παρατήρηση συνέβαλε στο να αποκλειστεί, με την χρήση υπολογιστών, η ύπαρξη 42-cap στο PG(4, 4).

Η διαδικασία είχε ως εξής:

Βήμα 1: Αρχικά καταγράφηκαν όλα τα πλήρη caps που είχαν 13, 14, 15, 16 ή 17 σημεία στο PG(3, 4), μέχρι ισομορφίας κάτω από την δράση της ΡΓL(4, 4). Θυμίζουμε ότι το 17-cap στο PG(3, 4) είναι μοναδικό, το ovoid, και έχει μελετηθεί.

Από φράγματα που έχουν δώσει οι Hirschfeld και Storme για τα πλήρη caps ([Hir3] και [Hir4]) γνωρίζουμε ότι δεν υπάρχουν πλήρη 15- και πλήρη 16- caps στο PG(3, 4). Αντίθετα από μια εργασία των Faina και Pambianco ([Fa]) γνωρίζουμε ότι υπάρχουν πλήρη 13- και πλήρη 14- caps. Με αυτά τα στοιχεία ολοκλήρωσαν την καταγραφή των ζητούμενων caps στο PG(3, 4).

Βήμα 2: Το δεύτερο και σημαντικότερο βήμα ήταν να εκτελεστεί ένα πρόγραμμα, το οποίο για κάθε cap με το λιγότερο 13 σημεία να ψάχνει για 42-caps που να τέμνουν ένα δεδομένο υπερεπίπεδο ενός δεδομένου cap τάξης 13. Το πρόγραμμα γράφτηκε σε C++. Χρειάζεται περίπου 1 MB μνήμη. Οι Edel και Bierbrauer έτρεξαν το πρόγραμμα σε ένα HP 712/60 και χρειάστηκαν από 17 ώρες όταν ξεκίνησαν από το ovoid στο PG(3, 4) μέχρι 19 μέρες όταν ξεκίνησαν με ένα 13-cap στο PG(3, 4).

Στην διεύθυνση http://www.math.uoc.gr/~marios/master/ μπορείτε να βρείτε μια τροποποιημένη έκδοση του προγράμματος που χρησιμοποίησαν οι Edel και Bierbrauer. Η καινούρια έκδοση γράφτηκε από τον Edel και τρέχει περίπου στο 1/10 του χρόνου που χρειάζονταν η αρχική έκδοση.

41-caps στο PG(4, 4)

Στο [BE] παρουσιάζονται και δύο 41-caps στο PG(4, 4) τα οποία δεν είναι προβολικά ισοδύναμα.

Αν συμβολίσουμε τα στοιχεία του σώματος $\mathbf{F}_4$ με 1, 2, 3, 4 όπου $2 + 3 = 2 \cdot 3 = 1$ τότε ένα 41-cap στο PG(4, 4) είναι οι στήλες του πίνακα

$$
\begin{array}{c}
10000213010223333122103103230321021023032 \\
01000132101013221322010121332022301101303 \\
00100303223220123321330101023302112102012 \\
00010032111103331223101030223133210010212 \\
00001130331132032231021013303320332120102
\end{array}
$$

Ο παραπάνω πίνακας είναι ο γεννήτορας πίνακας ενός $[41, 5, 28]_4$-κώδικα. Τα βάρη των κωδικών λέξεων κατανέμονται ως εξής:

$$A_{28} = 120,\ A_{29} = 360,\ A_{31} = 288,\ A_{32} = 135,\ A_{37} = 120.$$

Οι στήλες του παρακάτω πίνακα αποτελούν ένα άλλο 41-cap στο PG(4, 4)

$$
\begin{array}{c}
10000112213322333222333020022100311310012 \\
01000100200210110110130300230321231311222 \\
00100012002001101101103302003312213311222 \\
00010110011100011111111111111111111101011 \\
00001001111122222211133333300022222200113
\end{array}
$$

Τα βάρη των κωδικών λέξεων κατανέμονται ως εξής:

$$A_{24} = 9,\ A_{26} = 12,\ A_{28} = 105,\ A_{30} = 660,\ A_{32} = 90,\ A_{34} = 36,\ A_{36} = 51,\ A_{38} = 60.$$

Το 2003 ο Edel, σε προσωπική του επικοινωνία με τους υπόλοιπους συγγραφείς του [Bar], ανέφερε ότι υπάρχουν ακριβώς 2 διαφορετικά, μέχρι ισοδυναμίας, 41-caps στο PG(4, 4) διότι δεν προέκυψαν άλλα από την εκτέλεση του προγράμματος.

Σε προσωπική επικοινωνία που είχα με τον Edel στις αρχές του Σεπτέμβρη του 2004 επιβεβαίωσε αυτό το αποτέλεσμα το οποίο θα δημοσιευτεί, όπως ανέφερε, στο σύντομο μέλλον.

2.4.10 Ένα αναδρομικό άνω φράγμα για το $max_3(r, q)$

Το 1978 ο Hill στο [Hil3] έδωσε ένα γενικό αναδρομικό άνω φράγμα για την τιμή του $max_3(r, q)$. Θα ακολουθήσουμε τα βήματα που έκανε για την απόδειξή του.

Κάποιοι χρήσιμοι υπολογισμοί

Πριν προχωρήσουμε θα εισάγουμε κάποιους απαραίτητους συμβολισμούς και θα δώσουμε μια σειρά από λήμματα χρήσιμα για τις αποδείξεις των βασικών θεωρημάτων.

Συμβολισμός 2.4.10.1 Έστω q δοσμένη δύναμη πρώτου. Θα συμβολίζουμε

$$\theta_r := \frac{q^{r+1}-1}{q-1} = q^r + q^{r-1} + \ldots + q + 1.$$

Δεδομένου ενός [k, r + 1]-κώδικα C, θα συμβολίζουμε με M(C) έναν $k \times \theta_r$ πίνακα το οποίου στήλες είναι τα σημεία του C.

Δεδομένου ενός συνόλου $\{x_1, \ldots, x_{t+1}\}$ γραμμικά ανεξάρτητων κωδικών λέξεων του C θα συμβολίζουμε με $M(x_1, \ldots, x_{t+1})$ έναν $k \times \theta_r$ πίνακα το οποίου στήλες παράγονται από τα x_j.

Λήμμα 2.4.10.2 Έστω K ένα k-cap στο PG(r – 1, q) με κώδικα C. Τότε το ελάχιστο βάρος του C, όπως επίσης και τους κατάλοιπου κώδικα του C, είναι τουλάχιστον $k – m(r – 1, q)$.

Απόδειξη Βλ. θεώρημα 4.1 του [Hil3].

Λήμμα 2.4.10.3 Έστω C ένας προβολικός [k, r +1]-κώδικας με κατανομή βαρών $(w_1, w_2, \ldots, w_{\theta_r})$. Τότε

$$\sum_{i=1}^{\theta_r} w_i = kq^r \qquad (2.4.10.4)$$

$$\sum_{i=1}^{\theta_r} w_i^2 = kq^{r-1}[k(q-1)+1]. \qquad (2.4.10.5)$$

Απόδειξη Βλ. λήμμα 4.2 του [Hil3].

Ορισμός 2.4.10.6 Θέτουμε $m_1 = max_3(r – 1, q)$. Το θεώρημα 2.4.10.2 δείχνει ότι, για έναν cap-κώδικα, ισχύει $w_i \geq k – m_1$ για κάθε i. Οπότε μπορούμε να ορίσουμε τα **διορθωμένα βάρη** (amended weights) u_i ως εξής

$$u_i = w_i – (k – m_1)$$

Με αυτόν τον συμβολισμό τα $u_1 \geq u_2 \geq \ldots \geq u_{\theta_e} \geq 0$ θα είναι η **διορθωμένη κατανομή βαρών** (amended weight distribution).

Μπορούμε να ξαναδιατυπώσουμε το λήμμα 2.4.10.3 χρησιμοποιώντας τα διορθωμένα βάρη.

Λήμμα 2.4.10.7 Έστω C ένας προβολικός [k, r +1]-cap-κώδικας με διορθωμένη κατανομή βαρών $(u_1, u_2, \ldots, u_{\theta_e})$. Τότε

$$\sum_{i=1}^{\theta_r} u_i = m_1\theta_r - k\theta_{r-1}, \qquad \text{(B1)}$$

$$\sum_{i=1}^{\theta_r} u_i^2 = k^2\theta_{r-2} + k(q^{r-1} - 2m_1\theta_{r-1}) + m_1^2\,\theta_r. \qquad \text{(B2)}$$

Για έναν κατάλοιπο κώδικα C_1 του C με διορθωμένη κατανομή βαρών $(u_{11}, u_{12}, \ldots, u_{1\theta_{r-1}})$, έχουμε:

$$\sum_{i=1}^{\theta_{r-1}} u_{1i} = (m_1 - 1)\,\theta_{r-1} - (k-1)\,\theta_{r-2},$$

$$\sum_{i=1}^{\theta_{r-1}} u_{1i}^2 = (k-1)^2\,\theta_{r-3} + (k-1)[q^{r-2} - 2(m_1 - 1)\theta_{r-2}] + (m_1 - 1)^2\,\theta_{r-1}.$$

Παρατήρηση 2.4.10.8 Η τελευταία ισότητα ισχύει επειδή ο κατάλοιπος ενός cap-κώδικα είναι προβολικός κώδικας. Δεν ισχύει για γενικούς κώδικες.

Θεώρημα 2.4.10.9 Έστω C ένας [k, r + 1]-cap-κώδικας με κατανομή βαρών $(w_1, w_2, \ldots, w_{\theta_r})$ και διορθωμένη κατανομή βαρών $(u_1, u_2, \ldots, u_{\theta_r})$. Τότε

$$w_1 + w_2 \leq m_1(q-1) + k$$

και

$$u_1 + u_2 \leq m_1(q+1) - k \qquad \text{(2.4.10.10)}$$

Για έναν κατάλοιπο κώδικα του C ισχύει,

$$u_{11} + u_{12} \leq m_1 q - q + m_1 - k.$$

Απόδειξη Από το λήμμα 3.3 του [Hil3], κάθε στήλη του $k \times (q+1)$ πίνακα $M(x_1, x_2)$ έχει τουλάχιστον ένα μηδενικό. Επομένως, απαριθμώντας τα μηδενικά του $M(x_1, x_2)$,

$$(k - w_1) + (k - w_2) + \sum_{\substack{\lambda \in GF(q) \\ \lambda \neq 0}} [\,k - w(x_1 + \lambda w_2)] \geq k.$$

Από το λήμμα 2.4.10.2 ισχύει ότι $w(x_1 + \lambda x_2) \geq k - m_1$ για κάθε λ και επομένως

$$w_1 + w_2 \leq kq - (q - 1)(k - m_1) = m_1(q - 1) + k.$$

Άμεσα προκύπτει επομένως και ότι $u_1 + u_2 \leq m_1(q + 1) - k$.

Το αντίστοιχο αποτέλεσμα για τον κατάλοιπο κώδικα αποδεικνύεται ανάλογα.

Άνω φράγματα για το $\max_3(r, q)$

Πριν δώσουμε το ισχυρό άνω φράγμα είναι αναγκαίο να αποδείξουμε πρώτα κάποια ασθενέστερα αποτελέσματα.

Το πρώτο θεώρημα που θα δώσουμε είναι μια ελαφρώς τροποποιημένη έκδοση του θεωρήματος 5.1 του [Hil3].

Θεώρημα 2.4.10.11 Για κάθε $r \geq 3$ και $q \neq 2$ ισχύει

$$\max_3(r, q) \leq q \max_3(r - 1, q) - q + 1.$$

Απόδειξη Θα κάνουμε επαγωγή ως προς r. Παρατηρούμε ότι το θεώρημα ισχύει για r = 3, 4 (βλ. πίνακα 2). Υποθέτουμε ότι $r \geq 5$. Έστω $m_2 = \max_3(r, q)$ και $m_1 = \max_3(r - 1, q)$.

Έστω K ένα k-cap στο PG(r – 1, q) με κώδικα C. Ένας κατάλοιπος κώδικας C_1 του C είναι ένας προβολικός [k – 1, r]-κώδικας. Από το λήμμα 2.4.10.3 έχουμε ότι

$$\sum_{i=1}^{\theta_{r-1}} w_{1i} = (k - 1)q^{r-1}.$$

Από το λήμμα 2.4.10.2 έχουμε ότι $\sum_{i=1}^{\theta_{r-1}} w_{1i} \geq (k - m_1)\theta_{r-1}$. Οπότε,

$$(k - 1)q^{r-1} \geq (k - m_1)\theta_{r-1}.$$

Δηλαδή, $(q^{r-1} - \theta_{r-1})k \geq q^{r-1} - m_1\theta_{r-1}$. Από όπου προκύπτει $k \leq \dfrac{m_1\theta_{r-1} - q^{r-1}}{\theta_{r-1} - q^{r-1}}$.

Οπότε,

$$k \leq m_1 q + \frac{(m_1 - q^{r-1})(q-1)}{q^{r-1} - 1}.$$

Όμως για $q \neq 2$, από το επαγωγικό βήμα, έχουμε ότι

$$\max_3(5, q) \leq q \max_3(4, q) - q + 1 = q(q^2 + 1) - q + 1 = q^3 + 1$$

και

$$m_1 \le q^{r-2} + 1.$$

Οπότε,

$$k \le m_1 q + \frac{(q^{r-2} + 1 - q^{r-1})(q-1)}{q^{r-1} - 1} = m_1 q - q + 1 + \frac{q^{r-2}(q-1)}{q^{r-1} - 1}.$$

Από όπου προκύπτει

$$\max_3(r, q) \le q \max_3(r-1, q) - q + 1.$$

Παρατήρηση 2.4.10.12 Θυμίζουμε ότι ισχύει $\max_3(r, 2) = 2 \max_3(r-1, 2)$. Ακριβείς τιμές για το $\max_3(r, q)$ έχουμε επίσης για $r = 3, 4$. Επομένως, ενδιαφερόμαστε για φράγματα που ισχύουν για $q \neq 2$ και $r \ge 5$.

Στη συνέχεια θα βελτιώσουμε το προηγούμενο θεώρημα δείχνοντας ότι η ισότητα δεν ισχύει για κανένα $r \ge 5$.

Θεώρημα 2.4.10.13 Για $q \neq 2$ και $r \ge 5$ ισχύει

$$\max_3(r, q) \le q \max_3(r-1, q) - q.$$

Απόδειξη Όπως και πριν, θέτουμε $m_2 = \max_3(r, q)$ και $m_1 = \max_3(r-1, q)$. Έστω K ένα k-cap στο $PG(r-1, q)$ με $k = m_1 q - q + 1$ και C ένας κώδικας του K. Έστω C_1 ένα κατάλοιπος κώδικας του C με κατανομές βαρών $(u_{11}, u_{12}, .., u_{1\theta_{r-1}})$. Τότε από τις δύο τελευταίες εξισώσεις του λήμματος 2.4.10.7 έχουμε ότι

$$\sum_{i=1}^{\theta_{r-1}} u_{1i} = m_1 - 1 \qquad \text{(B3)}$$

$$\sum_{i=1}^{\theta_{r-1}} u_{1i}^2 = (m_1 - 1)[q^{r-1} - (q-1)(m_1 - 1)]. \qquad \text{(B4)}$$

Επειδή $\sum_{i=1}^{\theta_{r-1}} u_{1i}^2 \le \left(\sum_{i=1}^{\theta_{r-1}} u_{1i} \right)^2$ έπεται ότι $(m_1 - 1)[q^{r-1} - (q-1)(m_1 - 1)] \le (m_1 - 1)^2$.
Από όπου προκύπτει ότι $q^{r-1} - (q-1)(m_1 - 1) \le m_1 - 1$. Οπότε

$$m_1 \ge q^{r-2} + 1.$$

Αυτός όμως, από το θεώρημα 2.4.10.11, ισχύει μόνο αν

$$\max_3(s, q) = q^{s-1} + 1 \text{ για κάθε } s < r.$$

Για να αποδείξουμε το θεώρημα αρκεί να δείξουμε ότι $\max_3(5, q) \neq q^3 + 1$. Έστω, με σκοπό να καταλήξουμε σε άτοπο, ότι υπάρχει ένα $(q^3 + 1)$-cap K στο $PG(r-1, q)$. Τότε από τις σχέσεις (B3) και (B4) έχουμε ότι

$$\sum_{i=1}^{\theta_{r-1}} u_{1i} = q^3 \qquad \text{και} \qquad \sum_{i=1}^{\theta_{r-1}} u_{1i}^2 = q^3\,[q^4 - (q-1)q^3].$$

Οπότε,

$$\left(\sum_{i=1}^{\theta_{r-1}} u_{1i}\right)^2 = \sum_{i=1}^{\theta_{r-1}} u_{1i}^2 = q^6.$$

Η τελευταία σχέση μας δείχνει ότι $(u_{11}, u_{12}, \ldots) = (q^3, 0, 0, \ldots, 0)$. Από τη σχέση που συνδέει τα βάρη με τα διορθωμένα βάρη έχουμε ότι $u_{1i} = w_{1i} - (m_1 q - q + 1 - m_1) = w_{1i} - (m_1 - 1)(q-1) = w_{1i} - q^3(q-1) = w_{1i} - q^4 + q^3$. Από αυτό προκύπτει ότι για την κατανομή βαρών του C ισχύει

$$(w_{11}, w_{12,} w_{13}, \ldots) = (q^4, q^4 - q^3, q^4 - q^3, \ldots).$$

Άρα κάθε ένας από τους k κατάλοιπους του C περιέχει ένα διάνυσμα βάρους q^4. Επειδή κάθε διάνυσμα βάρους q^4 περιέχεται σε $(q^4 + 1) - q^4 = 1$ κατάλοιπους, υπάρχουν k διαφορετικά διανύσματα βάρους q^4 στον C. Πιο συγκεκριμένα,

$w_1 + w_2 = 2q^4$.

Αλλά, από την πρώτη σχέση του θεωρήματος 2.4.10.9 έχουμε ότι

$w_1 + w_2 \le m_1(q-1) + k = m_1(q-1) + (m_1 q - q + 1) = 2(q^3+1)q - q^3 - 1 - q + 1 = 2q^4 - q^3 + q < 2q^4$,

και φτάσαμε σε άτοπο.

Θα κάνουμε μια ακόμα βελτίωση του άνω φράγματος με την βοήθεια του επόμενου λήμματος το οποίο αποτελεί το πρώτο μέρος του λήμματος 5.4 του [Hil3].

Λήμμα 2.4.10.14 Έστω ότι $u_1, \ldots, u_n$ είναι πραγματικοί αριθμοί με

$$u_1 \ge u_2 \ge \ldots \ge u_n \ge 0.$$

Αν $u_1 + u_2 \le d$ και $u_1 < \frac{1}{2}\sum_{i=1}^{n} u_i$, τότε $\sum_{i=1}^{n} u_i^2 \le \frac{1}{2} d \sum_{i=1}^{n} u_i$, με την ισότητα να ισχύει αν και μόνο αν $u_i \in \{\frac{1}{2}d, 0\}$ για κάθε i με $1 \le i \le n$.

<u>Απόδειξη</u> Έστω $u_1 + u_2 \le d$ και $u_1 < \frac{1}{2}\sum_{i=1}^{n} u_i$. Αν $u_1 \le \frac{1}{2} d$, τότε $u_i \le \frac{1}{2} d$ για κάθε i οπότε και αποτέλεσμα είναι αληθές με την ισότητα να ισχύει αν και μόνο αν $\sum_{i=1}^{n}\left(u_i^2 - \frac{1}{2} d u_i\right) = 0$ δηλαδή αν και μόνο αν $u_1 = u_2 = \ldots = u_t = \frac{1}{2} d$ και $u_{t+1} = \ldots =$

$u_n = 0$ για κάποιο $1 \le t \le n$. Ας υποθέσουμε ότι $u_1 = \frac{1}{2}d + x$ όπου $x > 0$. Τότε για κάθε $i \ge 2$ ισχύει $u_i \le \frac{1}{2}d - x$. Επομένως,

$$\sum_{i=2}^{n} u_i^2 \le \left(\frac{1}{2}d - x\right)\sum_{i=2}^{n} u_i .$$

Οπότε,

$$\sum_{i=2}^{n} u_i^2 + u_1^2 - (\frac{1}{2}d + x)^2 \le \left(\frac{1}{2}d - x\right)[\sum_{i=2}^{n} u_i + u_1 - (\frac{1}{2}d + x)].$$

Δηλαδή,

$$\sum_{i=1}^{n} u_i^2 - (\frac{1}{2}d + x)^2 \le (\frac{1}{2}d - x)\,[\sum_{i=1}^{n} u_i - (\frac{1}{2}d + x)].$$

Συνεπώς,

$$\begin{aligned}\sum_{i=1}^{n} u_i^2 &\le \frac{1}{2}d\sum_{i=1}^{n} u_i + x\,(d + 2x - \sum_{i=1}^{n} u_i)\\ &= \frac{1}{2}d\sum_{i=1}^{n} u_i + x\,(2u_1 - \sum_{i=1}^{n} u_i)\\ &< \frac{1}{2}d\sum_{i=1}^{n} u_i \quad \text{διότι } u_1 < \frac{1}{2}\sum_{i=1}^{n} u_i \quad \text{και } x > 0.\end{aligned}$$

Τώρα μπορούμε να διατυπώσουμε το βασικό θεώρημα της παραγράφου

Θεώρημα 2.4.10.15 (Hill, 1978 στο [Hil3]) Για $q \ne 2$ και $r \ge 5$ ισχύει

$$\max_3(r, q) \le q \max_3(r - 1, q) - q - 1.$$

Απόδειξη Όπως και πριν ας υποθέσουμε ότι υπάρχει ένα $(qm_1 - q)$-cap K στο $PG(r - 1, q)$ για να καταλήξουμε σε άτοπο.

Από τις σχέσεις (B_1), (B_2) και (2.4.10.10) αντίστοιχα προκύπτει ότι τα διορθωμένα βάρη του C ικανοποιούν τις σχέσεις

$$\sum_{i=1}^{\theta_r} u_i = \theta_r + m_1 - 1, \qquad (2.4.10.4b)$$

$$\sum_{i=1}^{\theta_r} u_i^2 = -(q - 1)m_1^2 + (q^r + 2q)m_1 + \theta_r - q^r - q - 1, \qquad (2.4.10.5b)$$

$$u_1 + u_2 \le m_1 + q \qquad (2.4.10.10b)$$

Επειδή, $u_1 \le m_1 + q \le q^{r-2} + 1 + q < \frac{1}{2}(\theta_r + m_1 - 1) = \frac{1}{2}\sum_{i=1}^{n} u_i$, μπορούμε να εφαρμόσουμε το λήμμα 2.4.10.14 στην σχέση (2.4.10.10b) για να πάρουμε

$$\sum_{i=1}^{n} u_i^2 \le \frac{1}{2}(m_1 + q)\sum_{i=1}^{n} u_i .$$

Αντικαθιστώντας τα αθροίσματα με την βοήθεια των σχέσεων (2.4.10.4b) και (2.4.10.5b) έχουμε ότι

$$-(q-1)m_1^2 + (q^r + 2q)m_1 + \theta_r - q^r - q - 1 \le \frac{1}{2}(m_1 + q)(\theta_r + m_1 - 1)$$

Απλοποιώντας,

$$m_1^2(2q-1) + m_1(\theta_r - 1 - 2q^r - 3q) + (q^{r+1} - \theta_r + 2q^r + q + 1) \ge 0,$$

το οποίο μπορεί να ειδωθεί σαν πολυώνυμο δευτέρου βαθμού ως προς το m_1.

Από το θεώρημα 2.4.10.11 προκύπτει ότι $q^2 + 1 \le m_1 \le q^{r-2} + 1$.

Θεωρούμε την πραγματική συνάρτηση

$$f(x) = x^2(2q-1) + x(\theta_r - 1 - 2q^r - 3q) + (q^{r+1} - \theta_r + 2q^r + q + 1).$$

Θα αποδείξουμε ότι $f(x) < 0$ για κάθε $x \in [q^2 + 1, q^{r-2} + 1]$ από το οποίο θα καταλήξουμε και στο επιθυμητό άτοπο. Παρατηρούμε ότι η δεύτερη παράγωγος της $f(x)$ είναι $f''(x) = 2(2q-1) > 0$ άρα η $f(x)$ γίνεται μέγιστη για $x = q^2 + 1$ ή για $x = q^{r-2} + 1$. Άρα αρκεί να δείξουμε ότι οι τιμές $f(q^2 + 1)$ και $f(q^{r-2} + 1)$ είναι αρνητικές. Έχουμε:

$f(q^2 + 1) =$

$= (q^2 + 1)^2(2q-1) + (q^2 + 1)(\theta_r - 1 - 2q^r - 3q) + (q^{r+1} - \theta_r + 2q^r + q + 1)$

$= (q^2 + 1)^2(2q-1) + (q^2 + 1)\left(\frac{q^{r+1} - 1}{q-1} - 1 - 2q^r - 3q\right) + \left(q^{r+1} - \frac{q^{r+1} - 1}{q-1} + 2q^r + q + 1\right)$

$= \frac{1}{q-1}q^4(-q^{r-1} + 3q^{r-2} - q^{r-3} - 1) + 2q^5 - q^4 + 2q^3 - 2q^2 - 1.$

Για να ισχύει $f(q^2 + 1) < 0$ αρκεί να ισχύει

$$q^4(-q^{r-1} + 3q^{r-2} - q^{r-3} - 1) + (q-1)(2q^5 - q^4 + 2q^3 - 2q^2 - 1) < 0.$$

Δηλαδή αρκεί,

$$-q^{r+3} + 3q^{r+2} - q^{r+1} + 2q^6 - 3q^5 + 2q^4 - 4q^3 + 2q^2 - q + 1 < 0.$$

Επειδή στην τελευταία παράσταση τα πρόσημα είναι εναλλάξ και ο μεγαλύτερος συντελεστής είναι 4 η παράσταση είναι μικρότερη του μηδενός για κάθε $q \geq 5$ και $r \geq 5$.

Για $q = 4$ η παράσταση γράφεται $-4^{r+3} + 3\cdot 4^{r+2} - 4^{r+1} + 5405 = -5\cdot 4^{r+1} + 5405$ το οποίο είναι αρνητικό για κάθε $r \geq 6$.

Για $q = 3$ η παράσταση γράφεται $-3^{r+1} + 799$ και είναι αρνητική για κάθε $r \geq 7$.

Επομένως $f(q^2 + 1) < 0$ για $q \neq 2$ και $r \geq 5$ με μόνες εξαιρέσεις τα ζευγάρια $(r, q) = (5, 3), (5, 4), (6, 3)$.

Επίσης,

$f(q^{r-2} + 1) =$

$= (q^{r-2} + 1)^2 (2q - 1) + (q^{r-2} + 1)(\theta_r - 1 - 2q^r - 3q) + (q^{r+1} - \theta_r + 2q^r + q + 1)$

$$= (q^{r-2}+1)^2(2q-1)+(q^{r-2}+1)\left(\frac{q^{r+1}-1}{q-1} - 1 - 2q^r - 3q\right)+\left(q^{r+1} - \frac{q^{r+1}-1}{q-1} + 2q^r + q + 1\right).$$

Συνεπώς,

$$(q-1)\, f(q^{r-2} + 1) = -q^{2r-1} + 4q^{2r-2} - 3q^{2r-3} + q^{2r-4} + q^{r+2} - q^{r+1} + q^r - 4q^{r-1} + 2q^{r-2} - q + 1.$$

Το οποίο είναι αρνητικό για $q \neq 2$ και $r \geq 5$ με μόνες εξαιρέσεις τα ζευγάρια $(r, q) = (5, 4)$ και $(r, 3)$ για κάθε r.

Ας εξετάσουμε τώρα τις εξαιρέσεις.

(i) Για $(r, q) = (5, 4)$.

Έχουμε ότι $\max_3(5, 4) = 41$ και $\max_3(4, 4) = 4^2 + 1 = 17$ επομένως, το θεώρημα ισχύει αφού $41 \leq 4 \cdot 17 - 5 = 63$. Την εποχή που ο Hill δημοσίευσε το αποτέλεσμα η τιμή του $\max_3(5, 4)$ δεν ήταν γνωστή. Αν θεωρήσουμε την τιμή του $\max_3(5, 4)$ άγνωστη μπορούμε να εργαστούμε ως εξής:

Έστω ένα 64-cap στο PG(4, 4) με κώδικα C. Τότε, $\sum_{i=1}^{\theta_4} u_i = 357$ και $\sum_{i=1}^{\theta_4} u_i^2 = 3701$.

Επίσης, $u_1 + u_2 \leq 21$. Καταλήγουμε σε άτοπο λόγω του λήμματος 5.4 του [Hil3].

(ii) Για $(r, q) = (5, 3)$.

Έχουμε ότι $\max_3(5, 3) = 20$ και $\max_3(4, 3) = 3^2 + 1 = 10$ επομένως, το θεώρημα ισχύει.

(iii) Για $(r, q) = (r, 3)$ με $r \geq 6$ (την περίπτωση για $r = 5$ Την εξετάσαμε προηγουμένως).

Από το θεώρημα 2.4.10.13 για $r \geq 6$ ισχύει $\max_3(r-1, 3) \leq 20 \cdot 3^{r-6}$. Παρατηρούμε ότι $f(20 \cdot 3^{r-6}) = 2800 \cdot 9^{r-6} + (20 \cdot 3^{r-6})(3 - 2 \cdot 3^r) + (3^{r+1} - 9 + 2 \cdot 3^r + q + 1) < 0$ για $r \geq 6$ (όχι όμως και για $r = 5$). Το αποτέλεσμα προκύπτει όπως και στην γενική περίπτωση,

(iv) Για $(r, q) = (6, 3)$.

Έχουμε ότι $\max_3(6, 3) = 56$ και $\max_3(5, 3) = 20$ επομένως, το θεώρημα ισχύει.

Άρα το θεώρημα ισχύει σε κάθε περίπτωση.

Το θεώρημα 2.4.10.15 μπορεί να ξαναδιατυπωθεί ως εξής:

Θεώρημα 2.4.10.16 (Hill, 1978 στο [Hil3]) Για $q \neq 2$ και $s \geq 5$ ισχύει

$$\max_3(s + t, q) \leq q^t \max_3(s, q) - q^t - 2\theta_{t-1} + 1.$$

Απόδειξη Άμεση από το θεώρημα 2.4.10.6 κάνοντας επαγωγή ως προς t.

Παρατηρούμε ότι $\max_3(6, 3) = 56$ και $\max_3(5, 3) = 20$. Άρα ισχύει ότι

$$\max_3(6, 3) = 3 \cdot \max_3(5, 3) - 3 - 1.$$

Αυτό μας δείχνει ότι στο φράγμα που δώσαμε δεν μπορούν να γίνουν περαιτέρω βελτιώσεις στην γενική περίπτωση.

2.4.11 $112 \leq \max_3(7, 3) \leq 136$

Στην επόμενη διάσταση για q = 3 τα πιο γνωστά φράγματα είναι τα

$$112 \leq \max_3(7, 3) \leq 136$$

τα οποία μας δείχνουν ότι το πρόβλημα εύρεσης βέλτιστων caps στο PG(6, 3) είναι πολύ μακριά από την λύση του.

$\max_3(7, 3) \geq 112$

Από το 56-cap του Hill στο PG(5, 3) προκύπτει ένα 112-cap στο PG(6, 3) με τον ίδιο τρόπο όπου κατασκευάσαμε ένα 20-cap στο PG(4, 3) από ένα 10-cap στο PG(3, 3) (βλέπε παράγραφο 2.4.7). Αυτό μας δείχνει ότι $\max_3(7, 3) \geq 112$.

$\max_3(7, 3) \leq 136$

Εφαρμόζοντας το φράγμα που αποδείξαμε για το $\max_3(r, q)$ στην προηγούμενη παράγραφο για q = 3 και r = 7 έχουμε ότι $\max_3(7, 3) \leq 3 \cdot \max_3(6, 3) - 4 = 3 \cdot 56 - 4$. Δηλαδή ότι $\max_3(7, 3) \leq 164$.

Αρχικά, το 2000 στο [HLJSB] οι Hill, Landjev, Jones , Storme και Barát βελτίωσαν το άνω φράγμα στο 154 δείχνοντας ότι κάθε 53-cap στο PG(5, 3) περιέχεται σε ένα 56-cap και ότι υπάρχουν πλήρη 48-caps στο PG(5, 3).

Το 2002 οι Edel και Bierbrauer βελτίωσαν στο [BE4] ένα άνω φράγμα που είχε δώσει ο Meshulam για αφινικούς κώδικες στο [Me]. Με χρήση αυτού του φράγματος αποκλείστηκε η ύπαρξη ενός 149-cap στο PG(6, 3) και το άνω φράγμα για το $\max_3(7, 3)$ έπεσε στο 148. Για περισσότερες λεπτομέρειες για την απόδειξη ότι δεν υπάρχει 149-cap στο PG(6, 3) ο ενδιαφερόμενος αναγνώστης παραπέμπεται στην εισαγωγή (σελίδα 2) του [Bar].

Η βελτίωση του άνω φράγματος σε 136 έγινε το 2004, με τη χρήση ηλεκτρονικών υπολογιστών από κοινού από τους J. Barát, Y. Edel, R. Hill και L. Storme στο [Bar]. Στην εργασία τους έδειξαν ότι κάθε 49-cap στο PG(5,3) και κάθε 48-cap, το οποίο έχει ένα 20-υπερεπίπεδο με το πολύ 8-στερεά, περιέχονται σε ένα 56-cap. Αυτό βοήθησε να δώσουν μια γεωμετρική απόδειξη του ότι $\max_3(7, 3) \leq 137$. Στη συνέχεια έδειξαν ότι αν υπάρχει ένα 137-cap K στο PG(5,3) τότε υπάρχει ένα quadric το οποίο περιέχει τουλάχιστον 113 σημεία του K. Τέλος, παρατήρησαν ότι ένα quadric μπορεί να περιέχει το πολύ ένα 112-cap και έτσι κατέληξαν σε άτοπο. Αυτό ολοκλήρωσε και την απόδειξη.

2.4.12 $126 \leq \max_3(6, 4) \leq 153$

$\max_3(6, 4) \leq 153$

Η εύρεση της ακριβούς τιμής του $\max_3(5, 4)$ βοήθησε και στην βελτίωση των φραγμάτων για το $\max_3(6, 4)$. Σύμφωνα με το αναδρομικό τύπο του Hill (θεώρημα 2.4.10.15) ισχύει $\max_3(6, 4) \leq 4 \cdot 41 - 5$. Δηλαδή $\max_3(6, 4) \leq 159$. Από τον πίνακα 4.4(i) του [Hir4] φαίνεται ότι αυτό ήταν και το μικρότερο γνωστό άνω φράγμα μέχρι το 2001. Ωστόσο, σε επικοινωνία που είχε ο D. Glynn με τον T.A. Gulliver ο τελευταίος ανέφερε ότι κάνοντας απλή χρήση της Θεωρίας Κωδικοποίησης το άνω φράγμα μπορεί να μειωθεί σε 153.

Η απόδειξη είναι απλή. Ένα άνω φράγμα για την ελάχιστη απόσταση ενός $[153,147]_4$-κώδικα είναι το 3 το οποίο προκύπτει με την διαγραφή (το πολύ) 112 στηλών ενός γεννήτορα πίνακα του δυϊκού του. (Βλ. [Br]). Επομένως, δεν υπάρχει $[154, 148, 4]_4$-κώδικας.

Αν υπήρχε ένα 154-cap στο PG(5, 4) θα υπήρχε και ο αντίστοιχος $[153, 147, 4]_4$-κώδικας. Από εκεί προκύπτει ένας $[154, 148, 4]_4$-κώδικας το οποίο είναι άτοπο.

$\max_3(6, 4) \geq 126$

Χρησιμοποιώντας την απλή μέθοδο του διπλασιασμού μπορούν να προκύψουν δύο 82-caps στο PG(5, 4) από τα 41-caps στο PG(4, 4). Χρησιμοποιώντας την αναδρομική κατασκευή των Bierbrauer και Edel από το [BE2], η οποία αποτελεί μια βελτίωση της μεθόδου διπλασιασμού, μπορεί να προκύψει ένα 95-cap στο PG(5, 4).

Ο D. Glynn (στο [Gly]) έδειξε το 1999 την ύπαρξη ενός πλήρους 126-cap στο PG(5, 4) και του αντίστοιχου [126, 6, 88]-κώδικα. Στο ίδιο αποτέλεσμα κατέληξε και μια ομάδα ερευνητών αποτελούμενη από τους R.D. Baker, J.M. Dover, K.L. Wantz, G. Ebert (στο [Bak]) την ίδια χρονιά. Οι δύο μέθοδοι διαφέρουν στον τρόπο κατασκευής αλλά τα cap τα οποία κατασκεύασαν είναι ισόμορφα.

Ο Glynn χρησιμοποίησε ιδιότητες των κωνικών τομών του PG(2, 4). Τα βάρη των κωδικών λέξεων του κώδικα, που κατασκεύασε είναι 88, 96 και 120. Είναι δηλαδή ένας **κώδικας 3 βαρών**. Η ελάχιστη απόσταση του κώδικα είναι d = 88 η οποία είναι η καλύτερη γνωστή ελάχιστη απόσταση ενός $[126, 6]_4$-κώδικα. Η μόνη δυνατή άλλη ελάχιστη απόσταση είναι 92 η οποία προκύπτει από το φράγμα του Griesmer. Μέχρι σήμερα δεν έχει βρεθεί $[126, 6]_4$-κώδικας που να ικανοποιεί το φράγμα του Griesmer.

2.4.13 Γνωστά κάτω φράγματα για το $max_3(r, q)$ για $5 \le r \le 12$ και $q \le 9$

Θυμίζουμε ότι το πρόβλημα της εύρεσης του $max_3(r, q)$ έχει λυθεί πλήρως για $q = 2$ και για όλα τα r όπως επίσης έχει λυθεί για $r = 3$ και 4 για όλα τα q.

Μέχρι στιγμής τα γνωστά κάτω φράγματα για το $max_3(r, q)$ για $5 \le r \le 12$ και $q \le 9$ είναι τα εξής:

r\q	3	4	5	7	8	9
5	20*	41*	66	132	208	212
6	56*	126	186	434	695	840
7	112	288	675	2499	4224	6723
8	248	756	1715	6472	13520	17220
9	532	2110	4700	21555	45174	68070
10	1216	4938	17124	122500	270400	544644
11	2744	15423	43876	323318	878800	1411830
12	6464	34566	120740	1067080	2812160	5580100

Οι τιμές με αστερίσκο (*) είναι οι ακριβείς τιμές.

Στο [BE3] δείχνεται η κατασκευή ενός 66-cap στο PG(4, 5):

0100000004142323141423231414232341413232323214140000234141323214000
0010032044100320032001404411332224134321114422331423142332142341000
0001020211010202242443433333111103032323444400002443244312412114420
1111444411114444111144441111444422223333222233331144114422332233403
1111111111111111111111111111111111111111111111111111111111111111101

Στο [BE2] δείχνεται η κατασκευή $(q^4 + 2q^2)$-caps στο PG(6, q), καθώς και $q^2(q^2+1)^2$-caps στο PG(9, q). Αυτή η κατασκευή μας δίνει τα κάτω φράγματα για το $max_3(7, q)$ και $max_3(10, q)$. Για τα υπόλοιπα κάτω φράγματα βλ. [Ede].

2.4.14 Οι τιμές του $B_3(n, 4)$, για $5 \le n \le 112$

Κάνοντας χρήση των μέχρι σήμερα γνωστών αποτελεσμάτων για το $max_3(r, 3)$ μπορούμε να πάρουμε κάποιες επιπλέον τιμές για το $B_q(n, 4)$.

Θεώρημα 2.4.14.1

$$B_3(n, 4) = \begin{cases} 3^{n-4} & \text{για } 5 \le n \le 10 \\ 3^{n-5} & \text{για } 11 \le n \le 20 \\ 3^{n-6} & \text{για } 21 \le n \le 56 \\ 3^{n-7} & \text{για } 57 \le n \le 112 \end{cases}$$

2.4.15 Τελικές παρατηρήσεις

(1) Αναφέραμε στην αρχή του κεφαλαίου ότι το πρόβλημα προσδιορισμού του $\max_s$ (r, q) πρώτη φορά απασχόλησε τον Bose (1947). Δευτερεύουσας σημασία δουλειά έγινε από την Ιταλική Σχολή των γεωμετρών με πρωτοστάτες τους Segre, Barlotti και Tallini.

Για μια παρουσίαση των γνωστών αποτελεσμάτων που αφορούν στο $\max_s$ (r, q) και άλλες σχετικές συναρτήσεις, δείτε το [Hir1]. Για μια κατανοητή κάλυψη της θεωρίας των προβολικών γεωμετριών πάνω από πεπερασμένά σώματα δείτε το [Hir2].

(2) Για αποτελέσματα που αφορούν στο $\max_s$ (r, q) για $q = 3$ και $s \leq r \leq 15$ παραπέμπουμε τον ενδιαφερόμενο αναγνώστη στο [Ga].

(3) Δεν φαίνεται να υπάρχει κάποιος γενικός τύπος που να ακολουθούν τα αποτελέσματα του $\max_s$ (r, q) για συγκεκριμένες τιμές του d μεγαλύτερες από 4. Ωστόσο, όταν το d παίρνει τη μέγιστη τιμή του για δοσμένο r, δηλαδή όταν $d = r + 1$ εμφανίζεται ένα ενδιαφέρον pattern. Αυτή η περίπτωση είναι το αντικείμενο της επόμενης παραγράφου όπου θα δούμε συνοπτικά τα γνωστά αποτελέσματα μέχρι σήμερα.

(4) Μια άλλη εκδοχή του MLCT προβλήματος είναι η εύρεση, για δοσμένα q, n και k, η μέγιστη τιμή του d για την οποία υπάρχει ένας $[n, k, d]_q$-κώδικας. Αυτό θα είναι το αντικείμενο του επόμενου κεφαλαίου. Στην περίπτωση των δυαδικών γραμμικών κωδίκων οι Helgert και Stinaff (1973) δίνουν ένα πίνακα με τέτοιες τιμές (ή φράγματα όπου οι τιμές είναι άγνωστες) για $k \leq n \leq 127$. Για μια ανανεωμένη έκδοση αυτού του πίνακα, η οποία περιλαμβάνει πολλές βελτιώσεις από διάφορους συγγραφείς, ο ενδιαφερόμενος αναγνώστης μπορεί να δει τα [Ve], [Ve2] και [Bro].

2.5 Το MLCT πρόβλημα για d = r + 1

Όπως είδαμε από το φράγμα του Singleton η μεγαλύτερη τιμή που μπορεί να πάρει το d είναι r + 1. Θυμίζουμε ξανά ότι ένας $[n , n – r, r + 1]_q$-κώδικας ονομάζεται MDS. Τα μέχρι σήμερα γνωστά αποτελέσματα για τους MDS κώδικες υπαγορεύουν την διατύπωση της παρακάτω εικασίας η οποία είναι γνωστή ως η βασική εικασία για τους MDS κώδικες (main conjecture on MDS codes).

Εικασία 2.5.1 (Η βασική εικασία για τους MDS κώδικες) Αν $2 \leq r \leq q$ τότε

$$\max_r(r, q) = q + 1.$$

Μόνη εξαίρεση η περίπτωση όπου το $q = 2^h$ και r = 3 ή q – 1. Τότε ισχύει

$$\max_3(3, q) = \max_{q-1}(q – 1, q) = q + 2.$$

Στην περίπτωση όπου r > q ισχύει το ακόλουθο

Θεώρημα 2.5.2 Αν $r \geq q$ τότε

$$\max_r(r, q) = r + 1.$$

Επιπλέον, κάθε MDS κώδικας με $r \geq q$ είναι ισοδύναμος με έναν κώδικα επανάληψης μήκους r + 1.

Απόδειξη Ο κώδικας επανάληψης μήκους r + 1 είναι ένας $[r + 1, 1, r + 1]$-κώδικας με γεννήτορα πίνακα [11...1]. Οπότε,

$$\max_r(r, q) \geq r + 1.$$

Είναι προφανές ότι κάθε $[r + 1, 1, r + 1]$-κώδικας είναι ισοδύναμος με έναν κώδικα επανάληψης. Έστω $r \geq q$ και $\max_r(r, q) \geq r + 2$. Τότε υπάρχει ένας $[r + 2, 2, r + 1]_q$-κώδικας C. Για να έχει κάθε κωδική λέξη του C βάρος τουλάχιστον r + 1 πρέπει ο C να είναι ισοδύναμος με έναν κώδικα με γεννήτορα πίνακα

$$G = \begin{bmatrix} 1 & 0 & 1 & 1 & ... & 1 \\ 0 & 1 & a_1 & a_2 & ... & a_r \end{bmatrix},$$

όπου τα a_i είναι ανά δύο διαφορετικά μη-μηδενικά στοιχεία του $\mathbf{F}_q$. Συνεπώς, $r \leq q – 1$ και καταλήξαμε σε άτοπο.

Κάποιες βασικές προτάσεις σχετικά με την εικασία που διατυπώσαμε είναι οι εξής:

Πρόταση 2.5.3 Αν $2 \leq r \leq q$ τότε

$$\max_r(r, q) \geq q + 1.$$

Απόδειξη Βλ. πρόταση 15.5 του [Hil1].

Πρόταση 2.5.4 Ο δυαδικός ενός MDS κώδικα είναι MDS. Επιπλέον, υπάρχει MDS $[n, k]_q$-κώδικας αν και μόνο αν υπάρχει MDS $[n, n – k]_q$-κώδικας.

Απόδειξη

Ο κώδικας C με πίνακα ελέγχου ισοτιμίας $[A^T \mid I_r]$ είναι MDS $\Leftrightarrow$

Κάθε τετραγωνικός υποπίνακας του A^T έχει μη-μηδενική ορίζουσα (βλ. θεώρημα 15.6 του [Hil1]) $\Leftrightarrow$

Κάθε τετραγωνικός υποπίνακας του A έχει μη-μηδενική ορίζουσα $\Leftrightarrow$

Ο κώδικας $C^{\perp}$ με πίνακα ελέγχου ισοτιμίας $[I_{n-r} \mid A]$ είναι MDS.

Πρόταση 2.5.5 Αν $\max_r(r, q) = q + 1$ τότε $\max_{q+2-r}(q + 2 – r, q) = q + 1$.

Απόδειξη Έστω, για να καταλήξουμε σε άτοπο, ότι $\max_{q+2-r}(q + 2 – r, q) \geq q + 2$. Τότε υπάρχει ένας $[q +2, r, q + 3 – r]_q$-κώδικας του οποίου ο δυϊκός είναι ένας $[q +2, q + 2 – r, r + 1]_q$-κώδικας. Το οποίο είναι άτοπο γιατί υποθέσαμε ότι $\max_r(r, q) = q + 1$.

Πρόταση 2.5.6 Αν $q = 2^h$ και $r = q – 1$ τότε

$$\max_r(r, q) \geq q + 2.$$

Απόδειξη Βλ. πρόταση 15.9 του [Hil1].

Θυμίζουμε επίσης ότι για $q = 2^h$ ισχύει $\max_3(3, q) = q + 2$ (βλ .Θεώρημα 2.4.3.5).

Γνωστά αποτελέσματα που αφορούν στην εικασία 2.5.1

Η εικασία έχει αποδειχθεί για r = 2 (βλ. παράγραφο 2.3) και r = 3 (βλ. παράγραφο 2.4.2). Με γεωμετρικές μεθόδους αποδείχθηκε για r = 4 ([Se3]) και r = 5 ([Ca]) για όλα τα q. Λόγω της δυϊκότητας των MDS κωδίκων που αποδείξαμε παραπάνω η εικασία ισχύει για όλα τα r όπου $q – 3 \leq r \leq q$.

Με εξαντλητικό έλεγχο οι Maneri και Silverman (1966 στο [MaS]) και Jurick (1968 στο [Ju]) επιβεβαίωσαν την εικασία για $q \leq 11$ για όλα τα r. Στο [Hil5] αναφέρεται ότι καμία πρόοδος δεν έγινε από τότε μέχρι το 1989. Οι A.H. Ali, J.W.P. Hirschfeld, H. Kaneta το 1995 επιβεβαίωσαν την εικασία για q = 13 (στο [Ali]).

Τέλος, οι J. M. Chao και H. Kaneta, κάνοντας εξαντλητικό έλεγχο με την χρήση ηλεκτρονικών υπολογιστών, έδωσαν την απόδειξη της εικασίας για $q \leq 27$ για όλα τα r (1997 στο [CK1] και 2001 στο [CK2]).

Κεφάλαιο 3

Εύρεση και κατασκευή βέλτιστων γραμμικών κωδίκων δοσμένου μήκους

3.1 Εισαγωγή

Όπως αναφέραμε και στο προηγούμενο κεφάλαιο ένα κεντρικό πρόβλημα της θεωρίας κωδικοποίησης είναι η βελτιστοποίηση μιας εκ των παραμέτρων n, k και d για δοσμένες τιμές των άλλων δύο. Δύο εκδοχές, διαφορετικές από αυτές που είδαμε προηγουμένως, είναι οι ακόλουθες.

Πρόβλημα 1 Να βρεθεί το $d_q(n, k)$, η μεγαλύτερη τιμή του d για την οποία υπάρχει ένας $[n, k, d]_q$-κώδικας.

Πρόβλημα 2 Να βρεθεί το $n_q(k, d)$, η μικρότερη τιμή του n για την οποία υπάρχει ένας $[n, k, d]_q$-κώδικας.

Φυσικά, για δοσμένο q, η επίλύση του προβλήματος 1 για όλα τα n και k είναι ισοδύναμη με την επίλυση του προβλήματος 2 για όλα τα k και d.

Βασικό εργαλείο μας για την προσέγγιση του προβλήματος θα είναι το φράγμα του Griesmer (βλ. θεώρημα 1.1.2.11).

Μια μεγάλη κλάση κωδίκων που αγγίζουν το φράγμα του Griesmer είναι η κλάση των κωδίκων που ονομάζονται κώδικες τύπου BV. Τέτοιοι κώδικες δίνονται με συγκεκριμένο puncturing από πλεξίματα simplex κωδίκων και δείχνουν ότι, για δοσμένα q και k, το φράγμα του Griesmer επιτυγχάνεται για όλα τα επαρκώς μεγάλα d. Το επόμενο θεώρημα μας δίνει μια αναγκαία και ικανή συνθήκη για την ύπαρξη ενός κώδικα τύπου BV. Μια απόδειξη και αναλυτικά παραδείγματα υπάρχουν στα [Hil92], [MS].

Θεώρημα 3.1.1 (Belov, 1972) Για δοσμένα q, k και d γράφουμε

$$d = sq^{k-1} - \sum_{i=1}^{p} q^{u_i - 1}$$

όπου $s = \left\lceil \frac{d}{q^{k-1}} \right\rceil$, $k > u_1 \geq \ldots \geq u_p \geq 1$, και το πολύ $q - 1$ u_i παίρνουν κάποια δοσμένη τιμή. Τότε υπάρχει ένας $[g_q(k, d), k, d]$-κώδικας τύπου BV αν και μόνο αν

$$\sum_{i=1}^{\min(s+1,p)} u_i \leq sk.$$

Από το θεώρημα συμπεραίνουμε ότι το πρόβλημα 2 είναι μάλλον η πιο φυσική εκδοχή από τις δύο διότι το φράγμα του Griesmer μας εξασφαλίζει έναν σημαντικό κάτω φράγμα για το $n_q(k, d)$ το οποίο, για δοσμένες τιμές των q και k, επιτυγχάνεται για όλες τις αρκετά μεγάλες τιμές του d (βλ. παρακάτω). Οπότε, για δοσμένα q και k, η επίλυση του προβλήματος 2 για όλα τα d (ή η επίλυση του προβλήματος 1 για όλα τα n) είναι ένα πεπερασμένο πρόβλημα.

Στις επόμενες παραγράφους θα ασχοληθούμε με την επίλυση του προβλήματος 2 στις περιπτώσεις q = 2 και q = 4. Θα παρουσιάσουμε τα μέχρι σήμερα γνωστά αποτελέσματα.

3.2 Βέλτιστοι γραμμικοί κώδικες δοσμένης απόστασης στο GF(2)

Για δυαδικούς κώδικες το $n_2(k, d)$ είναι γνωστό για $k \leq 8$ και όλα τα d (Βλ. [Til3], [Bouy]). Ένας αναλυτικός πίνακας με φράγματα για το $d_2(n, k)$ δίνεται στο [Bro].

Θυμίζουμε ότι αν d περιττός τότε υπάρχει $[n, k, d]_2$-κώδικας αν και μόνο αν υπάρχει $[n + 1, k, d + 1]_2$-κώδικας (θεώρημα 2.4.1.1). Επομένως, στην περίπτωση των δυαδικών κωδίκων δοσμένου ενός k αρκεί να λύσουμε το πρόβλημα για όλα τα άρτια d.

Δύο ακόμα αποτελέσματα μας βοηθάνε να αποκλείσουμε αρκετές περιπτώσεις. Συγκεκριμένα,

Θεώρημα 3.2.1 (Logačev, 1974 στο [Log]) Αν $3 \leq d \leq 2^{k-2} - 2$, τότε

$$n_2(k, d) \geq g_2(k, d) + 1.$$

Θεώρημα 3.2.2 (van Tilborg, 1980 στο [Til2]) Αν $2^{k-2} + 3 \leq d \leq 2^{k-2} + 2^{k-3} - 4$, τότε

$$n_2(k, d) \geq g_2(k, d) + 1.$$

3.2.1 Βέλτιστοι δυαδικοί κώδικες διάστασης ≤ 6

Από το θεώρημα 3.1.1 στη περίπτωση όπου q = 2 έχουμε το ακόλουθο

Θεώρημα 3.2.1.1 (van Tilborg, 1980 στο [Til2]) Για κάθε $k \leq 7$ και για κάθε d ισχύει

$$n_2(k, d) = g_2(k, d)$$

εκτός πιθανόν από

$k = 5$ και $3 \leq d \leq 6$,
$k = 6$ και $3 \leq d \leq 14$ και $19 \leq d \leq 20$,
$k = 7$ και $3 \leq d \leq 30$, $35 \leq d \leq 44$, $67 \leq d \leq 72$.

Από το θεωρήματα 3.2.1, 3.2.2 και 3.2.1.1 αλλά και με χρήση του [Br] έχουμε τους ακόλουθους πίνακες:

d (άρτιος)	$n_2(5, d) - g_2(5, d)$
2	0
4 – 6	1
≥8	0

d (άρτιος)	$n_2(6, d) - g_2(6, d)$
2	0
4 – 14	1
16 – 18	0
20 – 30	1
≥ 32	0

3.2.2 Βέλτιστοι δυαδικοί κώδικες διάστασης 7

Θεώρημα 3.2.2.1 (i) $n_2(7, 4) = 12$, (ii) $n_2(7, 6) = 16$, (iii) $n_2(7, 4) = 12$, (iv) $n_2(7, 8) = 19$, (v) $n_2(7, 12) = 27$, (vi) $n_2(7, 24) = 50$, (vii) $n_2(7, 30) = 62$.

Απόδειξη Συνδυάζουμε τα θεωρήματα 3.2.1, 3.2.2 και 3.2.1.1 και κάνουμε χρήση του [Br].

Ισχύουν, επίσης τα επόμενα θεωρήματα:

Θεώρημα 3.2.2.2 (Alltop, 1976 στο [All]) (i) $n_2(7, 42) = 87$, (ii) $n_2(7, 44) = 90$.

Θεώρημα 3.2.2.3 (Farrell, 1978 στο [Far]) (i) $n_2(7, 36) = 75$, (ii) $n_2(7, 38) = 79$, (iii) $n_2(7, 40) = 82$.

Θεώρημα 3.2.2.4 (van Tilborg, 1978 στο [Til1]) $n_2(7, 20) = 43$.

Θεώρημα 3.2.2.5 (van Tilborg, 1981 στο [Til3]) (i) $n_2(7, 10) = 24$, (ii) $n_2(7, 14) = 32$, (iii) $n_2(7, 16) = 35$, (iv) $n_2(7, 18) = 40$, (v) $n_2(7, 22) = 47$, (vi) $n_2(7, 26) = 56$, (vii) $n_2(7, 28) = 59$, (iix) $n_2(7, 68) = 138$, (ix) $n_2(7, 70) = 142$, (x) $n_2(7, 72) = 145$.

Το τελευταίο θεώρημα ολοκλήρωσε και την καταγραφή των βέλτιστων δυαδικών κωδίκων διάστασης 7. Έχουμε τον παρακάτω πίνακα:

d	$g_2(7, d)$	$n_2(7, d)$
4	11	12
6	15	16
8	18	19
10	23	24
12	26	27
14	30	32
16	33	35
18	39	40
20	42	43
22	46	47
24	49	50

d	$g_2(7, d)$	$n_2(7, d)$
26	54	56
28	57	59
30	61	62
36	74	75
38	78	79
40	81	82
42	86	87
44	89	90
68	138	138
70	142	142
72	145	145

3.2.3 Βέλτιστοι δυαδικοί κώδικες διάστασης 8

Τον Ιούλιο του 2000 ολοκληρώθηκε και η καταγραφή των βέλτιστων δυαδικών κωδίκων διάστασης 8.

Μερικές πρόσφατες γνωστές τιμές του $n_2(8, d)$ φαίνονται στα ακόλουθα θεωρήματα

Θεώρημα 3.2.3.1 (Helleseth, Ytrehus, 1989 στο [Helle1]) $n_2(8, 14) = 33$.

Θεώρημα 3.2.3.2 (Helleseth, Ytrehus, 1990 στο [Helle2]) $n_2(8, 10) = 26$.

Θεώρημα 3.2.3.3 (Boukliev, Dodunekov, Helleseth, 1997 στο [Bouk]) (i) $n_2(8, 78) = 159$, (ii) $n_2(8, 80) = 162$.

Θεώρημα 3.2.3.4 (Bouyukliev, Jaffe, Vavrek, 2000 στο [Bouy]) (i) $n_2(8, 18) = 42$, (ii) $n_2(8, 26) = 58$, (iii) $n_2(8, 28) = 61$, (iv) $n_2(8, 30) = 65$, (v) $n_2(8, 34) = 74$, (vi) $n_2(8, 36) = 77$, (vii) $n_2(8, 38) = 81$, (iix) $n_2(8, 42) = 89$, (ix) $n_2(8, 60) = 124$.

Η απόδειξη του τελευταίου θεωρήματος έγινε με τη βοήθεια ηλεκτρονικών υπολογιστών με τη χρήση των προγραμμάτων Extension και Split που δημιούργησαν οι Bouyukliev και Jaffe αντίστοιχα.

Προέκυψε ο παρακάτω πίνακας:

d (άρτιος)	$n_2(8, d) - g_2(8, d)$
2	0
4 – 8	1
10 – 20	2
22 – 24	1
26 – 32	3
34 – 58	2
60	3

d (άρτιος)	$n_2(8, d) - g_2(8, d)$
62	1
64-66	0
68 – 92	1
94 – 98	0
100 – 104	1
≥ 106	0

Το πρόβλημα στις περιπτώσεις όπου $k \geq 9$ παραμένει ανοικτό μέχρι σήμερα.

3.3 Βέλτιστοι γραμμικοί κώδικες δοσμένης απόστασης στο GF(4)

Με το πρόβλημα για τετραδικούς κώδικες έχει καταπιαστεί κυρίως ο Hill. Στο [HN2] δίνονται οι τιμές του $n_3(k, d)$ για $k \leq 4$ για όλα τα d, και οι τιμές του $n_3(5, d)$ για όλες τις τιμές του d εκτός από 30.

Θα θεωρήσουμε το πρόβλημα για την περίπτωση των τετραδικών κωδίκων (q = 4). Στην παράγραφο 3.3.1 δίνουμε τα απαραίτητα προκαταρκτικά αποτελέσματα. Στην παράγραφο 3.3.2 λύνουμε το πρόβλημα της εύρεσης του $n_4(k, d)$ για $k \leq 3$ για όλα τα d και καθορίζουμε τις τιμές του $n_4(4, d)$, για όλες εκτός από 10, τις τιμές του d. Στην παράγραφο 3.3.3 δίνουμε, χωρίς αποδείξεις, τις υπόλοιπες 10 τιμές και στην παράγραφο 3.3.4 δίνουμε πίνακες για τα μέχρι τώρα γνωστά αποτελέσματα για το $n_4(5, d)$.

3.3.1 Προκαταρτικά αποτελέσματα

Όπου δεν αναφέρεται, αποδείξεις ή αναφορές για τα αποτελέσματα μπορούν να βρεθούν στην παράγραφο 2 του [HN2].

Το βάρος Hamming ενός διανύσματος x, το οποίο συμβολίζεται με w(x), είναι ο αριθμός των μη-μηδενικών συντεταγμένων του x. Για έναν γραμμικό κώδικα, η ελάχιστη απόσταση είναι ίση με το ελάχιστο από τα βάρη των μη-μηδενικών κωδικών λέξεών του. Αν C είναι ένας [n, k]-κώδικας με A_i και B_i θα συμβολίζουμε το πλήθος των κωδικών λέξεων με βάρος i στον C και τον δυϊκό κώδικα $C^{\perp}$, αντίστοιχα.

Θεώρημα 3.3.1.1 (Οι ταυτότητες του MacWilliams) Έστω C ένας $[n, k]_q$-κώδικας. Τότε τα A_i και B_i ικανοποιούν τις σχέσεις

$$\sum_{j=0}^{n-t} \binom{n-j}{t} A_j = q^{k-t} \sum_{j=0}^{t} \binom{n-j}{n-t} B_j \qquad (2.1)$$

για t = 0, 1, …, n.

Λήμμα 3.3.1.2 Για έναν $[n, k, d]_q$-κώδικα ισχύει $B_i = 0$ για κάθε τιμή του i, όπου $1 \leq i \leq k$, τέτοια ώστε δεν υπάρχει ένας $[n - i, k - i + 1, d]_q$-κώδικας.

Λήμμα 3.3.1.3 Έστω x και y δύο γραμμικά ανεξάρτητα διανύσματα του V(n, q). Τότε

$$w(x) + w(y) + \sum_{\lambda \in GF(q) \setminus \{0\}} w(x + \lambda y) = q(n - z(x, y)), \qquad (2.2)$$

όπου z(x, y) συμβολίζει το πλήθος των συντεταγμένων που είναι μηδέν ταυτόχρονα στο x και στο y.

Απόδειξη Θεωρούμε τον (q + 1) × n πίνακα M του οποίου γραμμές είναι τα διανύσματα του συνόλου $\{x, y, x + \lambda y \mid \lambda \in \mathbf{F}_q \setminus \{0\}\}$. Δηλαδή

$$M = \begin{bmatrix} x_1 & x_2 & \dots & x_n \\ y_1 & y_2 & \dots & y_n \\ x_1 + y_1 & x_2 + y_2 & \dots & x_n + y_n \\ x_1 + 2y_1 & x_2 + 2y_2 & \dots & x_n + 2y_n \\ \vdots & \vdots & \dots & \vdots \\ x_1 + (q-1)y_1 & x_2 + (q-1)y_2 & \dots & x_n + (q-1)y_n \end{bmatrix}$$

Παρατηρούμε ότι η i-οστή στήλη του πίνακα έχει μόνο μηδενικά αν $x_i = y_i = 0$ και ακριβώς ένα μηδενικό διαφορετικά. Μετρώντας το πλήθος των μηδενικών κατά στήλες και ύστερα κατά γραμμές προκύπτει το επιθυμητό αποτέλεσμα.

Πόρισμα 3.3.1.4 Έστω C ένας $[n, k, d]_q$-κώδικας με $k \geq 2$. Ισχύει:

$$A_i = 0 \text{ για } i > q(n - d).$$

Απόδειξη Έστω x μια μη-μηδενική κωδική λέξη του C. Επειδή $k \geq 2$ υπάρχει κωδική λέξη y η οποία δεν είναι βαθμωτό πολλαπλάσιο της x. Επειδή $w(y) \geq d$ από το προηγούμενο λήμμα έχουμε ότι $w(x) \leq qn - qd = q(n - d)$.

Πόρισμα 3.3.1.5 Έστω C ένας $[n, k, d]_4$-κώδικας με $k \geq 2$. Τότε

(i) Αν x και y είναι ένα γραμμικά ανεξάρτητο ζευγάρι κωδικών λέξεων του C τότε $w(x) + w(y) \leq 4n - 3d$,

(ii) $A_i = 0$ για $i > 4(n - d)$,

(iii) $A_i = 0$ ή 3 για $i > \frac{1}{2}(4n - 3d)$,

(iv) Αν $A_i > 0$ τότε $A_j = 0$ για $j > 4n - 3d - i$ και $i \neq j$.

(v) Έστω ότι ισχύει κάποιο από τα

(a) $w(x) \equiv 0$ ή 1 (mod 4) για όλα τα $x \in C$

(b) $w(x) \equiv 0$ ή 3 (mod 4) για όλα τα $x \in C$

Τότε το σύνολο $D = \{x \in C : w(x) \equiv 0 \pmod 4\}$ είναι γραμμικός υποκώδικας του C.

Απόδειξη Τα (i)-(iv) είναι αποτελέσματα ανάλογα με αυτά που δίνονται για κώδικες πάνω από το $\mathbf{F}_3$ στο [HN1] (πρόταση 2.14).

(i) Από το προηγούμενο λήμμα: $w(x) + w(y) = qn - qz(x, y) - \sum_{\lambda \in GF(q)\setminus\{0\}} w(x + \lambda y)$.

Συνεπώς, $w(x) + w(y) \leq 4n - 4d + d = 4n - 3d$.

(ii) Άμεσο από το προηγούμενο πόρισμα.

(iii) Έστω $i > \frac{1}{2}(4n - 3d)$. Από το (i) προκύπτει ότι δεν μπορούν να υπάρχουν δύο γραμμικά ανεξάρτητες κωδικές λέξεις βάρους i επομένως είτε δεν υπάρχει καμία κωδική λέξη βάρους είτε υπάρχουν 3 (οι x, 2x, 3x για κάποιο $x \in C$.

(iv) Άμεσο από το (i).

(v) Έστω $x, y \in D$. Τότε από την εξίσωση (2.2),

$$\sum_{i=1}^{3} w(x + iy) \equiv 0 \pmod 4.$$

Και στις δύο περιπτώσεις, (a) και (b), η μόνη περίπτωση να ισχύει η σχέση είναι $w(x + iy) \equiv 0 \pmod 4$ για i = 1, 2 και 3. Επομένως ο D είναι γραμμικός.

Λήμμα 3.3.1.6 (i) $n_q(k, d) \leq n_q(k, d + 1) - 1$
(ii) $n_q(k, d) \geq n_q(k, d - 1) + 1$.

Απόδειξη
(i) Έστω C ένας $[n, k, d + 1]$-κώδικας με $n = n_q(k, d + 1)$. Τότε με puncturing στον κώδικα (δηλαδή σβήνοντας μια συντεταγμένη) παίρνουμε έναν $[n, k - 1, d]$-κώδικα.

(ii) Άμεσο από το (i) αν θέσουμε όπου d το d – 1.

Λήμμα 3.3.1.7 Θεωρούμε C_1 έναν $[n_1, k, d_1]_q$-κώδικα και C_2 έναν $[n_2, k, d_2]_q$-κώδικα. Αν οι C_1 και C_2 έχουν γεννήτορες πίνακες G_1 και G_2 αντίστοιχα ο πίνακας $[G_1 \mid G_2]$ παράγει έναν $[n_1 + n_2, k, d_1 + d_2]$-κώδικα ο οποίος ονομάζεται **συναρμογή** (concatenation) των C_1 και C_2.

Ορισμός 3.3.1.8 Έστω G ένας γεννήτορας πίνακας ενός γραμμικού $[n, k, d]_q$-κώδικα C. Ο **κατάλοιπος κώδικας** (residual code) του C με βάση την κωδική λέξη c, ο οποίος συμβολίζεται με Res(C, c) είναι ο κώδικας που παράγεται από τον περιορισμό του G στις στήλες όπου η c είναι μηδέν.

Λήμμα 3.3.1.9 Έστω C ένας $[n, k, d]_q$-κώδικας και έστω κωδική λέξη $c \in C$ βάρους w, όπου $d > w\frac{q-1}{q}$. Τότε ο Res(C, c) είναι ένας $[n - w, k - 1, d^0]$-κώδικας με $d^0 \geq d - w + \left\lceil \frac{w}{q} \right\rceil$.

(Με $\lceil x \rceil$ συμβολίζουμε τον μικρότερο ακέραιο που είναι μεγαλύτερος ή ίσος από το x).

Πόρισμα 3.3.1.10 Έστω C ένας $[n, k, d]_q$-κώδικας και έστω κωδική λέξη $c \in C$ βάρους w. Τότε το Res(C, c) είναι ένας $[n - d, k - 1, \left\lceil \frac{d}{q} \right\rceil]$-κώδικας.

3.3.2 Βέλτιστοι τετραδικοί κώδικες διάστασης ≤ 4

Για ευκολία θα ονομάσουμε τα στοιχεία του σώματος $\mathbf{F}_4$ με 0, 1, 2, 3. Οι πράξεις θα γίνονται με βάση τους ακόλουθους πίνακες:

+	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

×	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

Για $k \le 2$ έπεται, από το θεώρημα 3.1.1, ότι $n_4(k, d) = g_4(k, d)$ για όλα τα d. Οπότε

$$n_4(1, d) = d \text{ και } n_4(2, d) = d + \left\lceil \frac{d}{4} \right\rceil \text{ για όλα τα d.}$$

Για $k = 3$ και $k = 4$ το θεώρημα 3.1.1 μας δίνει ότι $n_4(3, d) = g_4(3, d)$ για $d \ge 9$, και ότι $n_4(4, d) = g_4(4, d)$ για $45 \le d \le 64$ και για $d \ge 81$. Οι εναπομένουσες τιμές του d βρίσκονται στους πίνακες 1 και 2, μαζί με τα μέχρι τώρα καλύτερα φράγματα για τις τιμές του $n_4(k, d)$ για $k = 3$ και 4 αντίστοιχα. Για σύγκριση, συμπεριλαμβάνουμε και τις αντίστοιχες τιμές του φράγματος του Griesmer.

Σε αυτούς τους πίνακες η ένδειξη i αναφέρεται στο θεώρημα 3.3.2.i των επόμενων σελίδων. Τα άνω φράγματα χωρίς ένδειξη δίνονται από puncturing κάποιου κώδικα (λήμμα 3.3.1.5(i)). Τα κάτω φράγματα χωρίς ένδειξη δίνονται ή από το φράγμα του Griesmer (θεώρημα 1.1.2.11) ή από το λήμμα 3.3.1.5(ii).

Πίνακας 1 – Τιμές για το $n_4(3, d)$

d	$g_4(3, d)$	$n_4(3, d)$
1	3	3
2	4	4
3	5	5
4	6	6 [1]
5	8	8
6	9	9 [1]
7	10	11 [2]
8	11	12 [1]

Πίνακας 1 – άνω φράγματα (κατασκευές)

Θεώρημα 3.3.2.1 (i) $n_4(3, 4) \le 6$, (ii) $n_4(3, 6) \le 9$, (iii) $n_4(3, 8) \le 12$.

Απόδειξη (i) Ο πίνακας $\begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 2 & 3 \\ 0 & 0 & 1 & 1 & 3 & 2 \end{bmatrix}$

παράγει έναν $[6, 3, 4]_4$-κώδικα.

(ii) Ένας [9, 3, 6]-κώδικας δίνεται από shortening του [10, 4, 6]-κώδικα που δίνεται στον πίνακα 2.
(iii) Ένας [12, 3, 8]-κώδικας δίνεται από shortening του [13, 4, 8]-κώδικα που δίνεται στον πίνακα 2.

Πίνακας 1 – κάτω φράγμα (μη-ύπαρξη)

Θεώρημα 3.3.2.2 $n_4(3, 7) > 10$.

Απόδειξη Έστω, με σκοπό να φτάσουμε σε άτοπο, ότι υπάρχει κάποιος $[10, 3, 7]_4$-κώδικας C. Επειδή δεν υπάρχουν [9, 3, 7] και [8, 2, 7] κώδικες στο $\mathbf{F}_4$ (για d = 7, από το φράγμα, του Griesmer το ελάχιστο n για το οποίο υπάρχει κώδικας με k = 3 και k = 2 είναι 11 και 9 αντίστοιχα) από το λήμμα 3.3.2 έπεται ότι $B_1 = B_2 = 0$. Οι πρώτες τρεις ταυτότητες του MacWilliams (θεώρημα 3.3.1) για n = 10 και k = 3 γίνονται ως εξής:

Για t = 0: $\sum_{j=0}^{10} A_j = 4^3$.

Για t = 1: $\sum_{j=0}^{9} \binom{10-j}{1} A_j = 16 \cdot \sum_{j=0}^{1} \binom{10-j}{9}$

Για t = 2: $\sum_{j=0}^{8} \binom{10-j}{2} A_j = 4 \cdot \sum_{j=0}^{2} \binom{10-j}{8}$

Προκύπτει το σύστημα

$A_7 + A_8 + A_9 + A_{10} = 63$
$A_8 + 2A_9 + 3A_{10} = 39$
$A_9 + 3\,A_{10} = 24$

Έχοντας υπ' όψιν ότι κάθε A_i πρέπει να είναι μη-αρνητικό πολλαπλάσιο του 3 (επειδή αν το x είναι μια μη-μηδενική κωδική λέξη τότε είναι επίσης και το 2x και το 3x και όλες έχουν το ίδιο βάρος) οι μόνες λύσεις είναι

$A_{10} = 6$, $A_9 = 6$, $A_8 = 9$, $A_7 = 42$

και

$A_{10} = 3$, $A_9 = 15$, $A_8 = 0$, $A_7 = 45$

Η πρώτη περίπτωση αποκλείεται από το πόρισμα 3.3.1.4(iii) αφού για i > 9 πρέπει $A_i = 0$ ή 3 αλλά στην πρώτη περίπτωση έχουμε $A_{10} = 6$. Αν υπάρχει επομένως $[10, 3, 7]_4$-κώδικας C τα βάρη των κωδικών του λέξεων του θα πρέπει να ικανοποιούν την δεύτερη περίπτωση. Έστω λοιπόν δύο κωδικές λέξεις x και y του C γραμμικά ανεξάρτητες και βάρους 9 (υπάρχουν τέτοιες αφού $A_9 > 3$). Από το λήμμα 3.3.1.3 έχουμε ότι $9 + 9 + \sum_{\lambda=1}^{3} w(x + \lambda y) = 4(10 - z)$. Δηλαδή $\sum_{\lambda=1}^{3} w(x + \lambda y) = 22 - 4z$. Η τελευταία σχέση είναι αδύνατη αφού τα μόνα δυνατά βάρη είναι 7, 9 και 10.

Παρατήρηση Το τελευταίο αποτέλεσμα μπορεί να προκύψει και εναλλακτικά ως εξής. Επειδή $B_2 = 0$, οι στήλες του γεννήτορα πίνακα του C μπορεί να θεωρηθούν σαν ένα σύνολο K από 10 προβολικά διακεκριμένα σημεία του προβολικού επιπέδου PG(2, 4). Επειδή κάθε κωδική λέξη έχει το πολύ 3 μηδενικά, το K τέμνει κάθε ευθεία του PG(2, 4) το πολύ σε 3 σημεία. Με άλλα λόγια το K είναι ένα 10-cap στο PG(2, 4) το οποίο είναι άτοπο αφού $\max_3(3, 4) = 6$ (βλ. θεώρημα 2.4.2.6 στην παράγραφο 2.4 αλλά και [10, πόρισμα 1 του θεωρήματος 12.2.3]).

Στην πραγματικότητα, στην 3-διάστατη περίπτωση τα γνωστά αποτελέσματα για τα (n, t)-caps μπορούν να χρησιμοποιηθούν για την εύρεση του $n_q(3, d)$ για όλα τα d, για όλα τα σώματα μέχρι q = 8. Περισσότερες λεπτομέρειες μπορείτε να βρείτε στο [Hil92].

Πίνακας 2 – Τιμές και φράγματα για το $n_4(4, d)$

d	$g_4(4, d)$	$n_4(4, d)$	d	$g_4(4, d)$	$n_4(4, d)$
1	4	4	33	46	46
2	5	5^{3}	34	47	47
3	6	7^{6}	35	48	48
4	7	8	36	49	49^{3}
5	9	9	37	51	51 – 52
6	10	10	38	52	52 – 53
7	11	12	39	53	54^{11}
8	12	13	40	54	55^{3}
9	14	14	41	56	56 – 57
10	15	15	42	57	57 – 58
11	16	16	43	58	59^{12}
12	17	17^{3}	44	59	60^{3}
13	19	20^{8}			
14	20	21			
15	21	22			
16	22	23^{3}			
17	25	25	65	89	89
18	26	26	66	90	90
19	27	27	67	91	91
20	28	28^{3}	68	92	92^{5}
21	30	30	69	94	94
22	31	31^{3}	70	95	95^{5}
23	32	33^{9}	71	96	96 – 97
24	33	34^{5}	72	97	97 – 98
25	35	36^{10}	73	99	99
26	36	37	74	100	100
27	37	38	75	101	101
28	38	39^{3}	76	102	102^{5}
29	40	41^{10}	77	104	104 – 105
30	41	42	78	105	105 – 106
31	42	43	79	106	106 – 107
32	43	44^{4}	80	107	$107 – 108^{5}$

Πίνακας 2 – άνω φράγματα (κατασκευές)

Αρχικά δίνουμε κάποιες σποραδικές κατασκευές [n, 4, d]-κωδίκων στο $\mathbf{F}_4$.

Θεώρημα 3.3.2.3 (i) $n_4(4, 2) \leq 5$, (ii) $n_4(4, 6) \leq 10$, (iii) $n_4(4, 12) \leq 17$, (iv) $n_4(4, 16) \leq 23$, (v) $n_4(4, 20) \leq 28$, (vi) $n_4(4, 22) \leq 31$, (vii) $n_4(4, 28) \leq 39$, (viii) $n_4(4, 36) \leq 49$, (ix) $n_4(4, 40) \leq 55$, (x) $n_4(4, 44) \leq 60$.

Απόδειξη

(i) Ο κώδικας $\{(x_1, x_2, x_3, x_4, x_5) \in V(5, 4) \mid \sum_{i=1}^{5} x_i = 0\}$ είναι ένας $[5, 4, 2]_4$-κώδικας.

(ii) Στο [As] δείχνεται ότι ο εκτεταμένος QR $[12, 6]_4$-κώδικας έχει ελάχιστη απόσταση 6. Εφαρμόζοντας shortening δύο φορές παίρνουμε έναν $[10, 4, 6]_4$-κώδικα.

(iii) Τα σημεία ενός ελλειπτικού quadric στο PG(3, q) σχηματίζουν ένα $(q^2 + 1)$-σύνολο K το οποίο τέμνει κάθε επίπεδο σε 1 ή q + 1 σημεία. Οπότε ο πίνακας του οποίου οι στήλες είναι τα σημεία του K παράγει έναν $[q^2 + 1, 4, q^2 – q]$-κώδικα του οποίου οι μη-μηδενικές κωδικές λέξεις έχουν βάρος 2. Αυτός ο κώδικας δίνεται ως το παράδειγμα TF3 στο [Cald]. Επειδή $g_q(4, q^2 – q) = (q^2 – q) + (q – 1) + 1 + 1 = q^2 + 1$ αυτός ο κώδικας ικανοποιεί το φράγμα του Griesmer για κάθε q. Συγκεκριμένα, υπάρχει $[17, 4, 12]_4$-κώδικας.

(iv) Έστω G_1 ένας γεννήτορα πίνακας ενός [17, 4, 12]-κώδικα, όπως τον περιγράψαμε στο (iii), ο οποίος έχει μια κωδική λέξη βάρους 16 ως τελευταία γραμμή. Έστω G_2 ο γεννήτορα πίνακας ενός [6, 3, 4]-κώδικα. Τότε ο πίνακας

$$\left[\begin{array}{c|c} G_1 & \begin{matrix} G_2 \\ \hline 0 \;\; 0 \;\; 0 \;\; 0 \;\; 0 \;\; 0 \end{matrix} \end{array}\right]$$

προφανώς παράγει έναν [23, 4, 16]-κώδικα.

(v) Μπορεί να αποδειχτεί (με μεθόδους οι οποίες θα χρησιμοποιηθούν αργότερα για την απόδειξη της μη-ύπαρξης κάποιων κωδίκων) ότι αν υπάρχει ένας $[28, 4, 20]_4$-κώδικας τότε η μοναδική πιθανή κατανομή των βαρών των λέξεών του είναι $A_{20} = 189$, $A_{24} = 63$, $A_{28} = 3$. Με τη χρήση υπολογιστή αναζητήσαμε κώδικα με αυτή την κατανομή και βρήκαμε έναν [28, 4, 20]-κώδικα με γεννήτορα πίνακα

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

(vi) Ένας [31, 4, 22]-κώδικας κατασκευάζεται στο [Hil78]. Ο γεννήτορας πίνακάς του είναι

0 0 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
1 0 0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 2 2 2 2 2 2 2 3 3 3 3 3 3 3
0 1 0 0 1 1 2 2 3 3 1 0 0 3 3 2 2 3 2 2 1 1 0 0 2 3 3 0 0 1 1
0 0 1 0 0 1 2 3 1 2 3 0 2 0 1 1 3 2 0 1 2 3 1 3 0 0 3 2 3 1 2

και η κατανομή των βαρών του είναι $A_{22} = 141$, $A_{24} = 87$, $A_{28} = 24$, $A_{30} = 30$.

(vii) Ένας [39, 4, 28]-κώδικας δίνεται με shortening του [40, 5, 28]-κώδικα που παρουσιάζουμε στο θεώρημα 3.3.2.4.

(viii) Μπορεί να αποδειχθεί ότι αν υπάρχει ένας [49, 4, 36]-κώδικας τότε έχει μια από τις δύο ακόλουθες κατανομές βαρών:

$$A_{36} = 204, \qquad A_{40} = 48, \qquad A_{48} = 3,$$

ή

$$A_{36} = 207, \qquad A_{40} = 39, \qquad A_{44} = 9,$$

Με την υπόθεση ότι ο κώδικας έχει την πρώτη κατανομή βαρών, ο ακόλουθος γεννήτορας πίνακας κατασκευάστηκε με το χέρι. Στη συνέχεια ελέγχθηκε από υπολογιστή ότι πράγματι αυτός ο πίνακας παράγει τον κώδικα που θέλουμε.

11111111111111111111111111111111111111111111111110
11111111111122222222222233333333333330000000001
11122233300001112223330000111222333000011122233 30
01302301201230120130320123023021031012312312312 30

(xi), (x) Υπάρχει μια κλάση κωδίκων στο $\mathbf{F}_q$ με όλες τις μη-μηδενικές λέξεις να έχουν βάρους 2 και με παραμέτρους $[i(q + 1), 4, (i – 1)q]$ για $i = 2, 3, \ldots, q^2$. Αυτά είναι τα παραδείγματα SU2 στο [Cald]. Παίρνοντας $q = 4$, $i = 10$ και 11 προκύπτει ένας [55, 4, 40]-κώδικας και ένας [60, 4, 44]-κώδικας, αντίστοιχα, στο $\mathbf{F}_4$.

Θεώρημα 3.3.2.4 Υπάρχουν κώδικες πάνω από το $\mathbf{F}_4$ με παραμέτρους [44, 4, 32] και [40, 5, 28].

Απόδειξη Ένας πίνακας της μορφής

$$[G_1 \mid G_2 \mid \ldots \mid G_t],$$

όπου κάθε G_i είναι ένας **κυκλοτερής** (circulant)[2] $k \times k$ πίνακας, μπορεί να χρησιμοποιηθεί για να παράγουμε ένα [kt, k]-κώδικα ο οποίος είναι γνωστός σαν **σχεδόν-κυκλικός κώδικας** (quasi-cyclic code). Εξαντλητικές έρευνες με υπολογιστή για τέτοιους [4t, 4]-κώδικες στο $\mathbf{F}_4$ οι οποίοι να έχουν τη μέγιστη δυνατή ελάχιστη απόσταση έγιναν από τον Greenough [Gre1], ο οποίος βρήκε

[2] Ένας πίνακας είναι **κυκλοτερής** αν οι γραμμές του προκύπτουν από κυκλική μετάθεση της πρώτης γραμμής.

κώδικες με παραμέτρους [8, 4, 4], [12, 4, 7], [16, 4, 11], [20, 4, 13], [24, 4, 16], [28, 4, 19], [32, 4, 22], [36, 4, 25], [40, 4, 28], [44, 4, 32] και [48, 4, 35]. Πολλοί από αυτούς του κώδικες έπιασαν ήδη γνωστά άνω φράγματα του πίνακα 2 και ο [44, 4, 32]-κώδικας έδωσε ένα νέο φράγμα. Σχεδόν-κυκλικοί κώδικες με τις ίδιες παραμέτρους βρέθηκαν όμοια και ανεξάρτητα από τους Gulliver και Bhargava [Gul]. Επιπλέον, το [Gul] δίνει επίσης αποτελέσματα ερευνών σε μεγαλύτερες διαστάσεις, συμπεριλαμβανομένης και της κατασκευής ενός [40, 5, 28]-κώδικα τον οποίο χρησιμοποιούμε στην απόδειξη του θεωρήματος 3.3.2.3(vii).

Οι κώδικες τύπου [44, 4, 32] και [40, 5, 28] παράγονται από πίνακες τις παραπάνω μορφής των οποίων οι πρώτες γραμμές είναι αντίστοιχα

(1000 1100 2100 1010 2110 1210 2210 2111 2211 2311 3121),

(1000 10120 11020 11230 12220 13130 13210 11312).

Πίνακας 3

C_1	C_2	C
[17, 4, 12]	[17, 4, 12]	[34, 4, 24]
[28, 4, 20]	[64, 4, 48]	[92, 4, 68]
[10, 4, 6]	[85, 4,64]	[95, 4, 70]
[17, 4, 12]	[85, 4, 64]	[102, 4, 76]
[44, 4, 32]	[64, 4, 48]	[108, 4, 80]

Θεώρημα 3.3.2.5 $n_4(4, 24) \leq 34$, $n_4(4, 68) \leq 92$, $n_4(4, 70) \leq 95$, $n_4(4, 76) \leq 102$, $n_4(4, 80) \leq 108$.

Απόδειξη Οι παραπάνω κώδικες C μπορούν να κατασκευαστούν με συναρμογή (concatenation) (λήμμα 3.3.1.7) όπως φαίνεται στον πίνακα 3. Όλοι οι κώδικες C_1 και C_2 που χρειαζόμαστε είτε έχουν κατασκευαστεί παραπάνω είτε είναι τύπου BV (θεώρημα 3.1.1).

Θεώρημα 3.3.2.6 $n_4(4, 3) > 6$.

Απόδειξη Έστω ότι υπάρχει ένας $[6, 4, 3]_4$-κώδικας C . Τότε ο C είναι ισοδύναμος με ένα κώδικα που έχει γεννήτορα πίνακα

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & a_1 \\ 0 & 1 & 0 & 0 & 1 & a_2 \\ 0 & 0 & 1 & 0 & 1 & a_3 \\ 0 & 0 & 0 & 1 & 1 & a_4 \end{bmatrix}$$

όπου τα a_1, a_2, a_3, a_4 είναι μη-μηδενικά αλλιώς ο κώδικας θα είχε ελάχιστη απόσταση μικρότερη από 3. Τουλάχιστον δύο από τα a_i πρέπει να ταυτίζονται. Οπότε έχουμε απόσταση 2 μεταξύ των αντίστοιχων στηλών του G, το οποίο είναι άτοπο.

Θεώρημα 3.3.2.7 $n_4(4, 7) > 11$.

Απόδειξη Έστω ότι υπάρχει ένας $[11, 4, 7]_4$-κώδικας C. Τότε ένας shortened κώδικας του C είναι ένας $[10, 3, 7]_4$-κώδικας. Τέτοιος κώδικας δεν υπάρχει σύμφωνα με τον πίνακα 1.

Θεώρημα 3.3.2.8 $n_4(4, 13) > 19$.

Απόδειξη Υποθέτουμε ότι υπάρχει ένας $[19, 4, 14]_4$-κώδικας C. Από το λήμμα 3.3.1.2 έχουμε ότι $B_1 = B_2 = B_3 = 0$ (επειδή δεν υπάρχουν κώδικες με παραμέτρους $[18, 4, 13]_4$, $[17, 3, 13]_4$ ή $[16, 2, 13]_4$ λόγω του φράγματος του Griesmer). Από το λήμμα 3.3.1.9 ο κατάλοιπος κώδικας του C με βάση μια κωδική λέξη βάρους 17 θα είναι ένας $[2, 3, 1]_4$-κώδικας ο οποίος προφανώς δεν υπάρχει. Επομένως $A_{17} = 0$. Οι πρώτες τέσσερις ταυτότητες του MacWilliams (θεώρημα 3.3.1.1), μετά από αναγωγή ομοίων όρων, γίνονται ως εξής:

$A_{13} + A_{14} + A_{15} + A_{16} + A_{18} + A_{19} = 255,$
$A_{14} + 2A_{15} + 3A_{16} + 5A_{18} + 6A_{19} = 333,$
$A_{15} + 3A_{16} + 10A_{18} + 15A_{19} = 405,$
$A_{16} + 10A_{18} + 20A_{19} = 483.$

Οι τελευταίες δύο εξισώσεις δίνουν

$A_{15} + 2A_{16} = 5A_{19} - 78,$

Το οποίο είναι αδύνατο επειδή $A_{19} = 0$ ή 3 από το πόρισμα 3.3.1.5(iii).

Θεώρημα 3.3.2.9 $n_4(4, 23) > 32$.

Απόδειξη (Η μη ύπαρξη ενός $[32, 4, 23]_4$-κώδικα αποδείχτηκε στο [Hil78], η απόδειξη καλύπτει τρεις σελίδες. Μια ελαφρώς μικρότερη γεωμετρική απόδειξη δόθηκε στο [Bram]. Η ακόλουθη απόδειξη, η οποία δίνεται με όρους της θεωρίας κωδικοποίησης, είναι και αυτή με τη σειρά της ελαφρώς μικρότερη).

Υποθέτουμε ότι υπάρχει ένας $[32, 4, 23]_4$-κώδικας C.

Από το λήμμα 3.3.1.2 επειδή δεν υπάρχουν $[31, 4, 23]_q$ και $[30, 3, 23]_q$-κώδικες για οποιοδήποτε q (για d = 23 το ελάχιστο n για το οποίο υπάρχει κώδικας με k = 4 και k =3 είναι 33 και 31 αντίστοιχα) έπεται ότι $B_1 = B_2 = 0$.

Από το λήμμα 3.3.1.9 έχουμε ότι $A_{25} = A_{29} = A_{30} = 0$. Οι ταυτότητες του MacWilliams, μετά από αναγωγές, γίνονται

(a) $A_{23} + A_{24} + A_{26} + A_{27} + A_{28} + A_{31} + A_{32} = 255,$
(b) $A_{24} + 3A_{26} + 4A_{27} + 5A_{28} + 8A_{31} + 9A_{32} = 279,$
(c) $3A_{26} + 6A_{27} + 10A_{28} + 28A_{31} + 36A_{32} = 492,$
(d) $3A_{27} + 10A_{28} + 70A_{31} + 108A_{32} = 3012 - 6B_2,$

Από το πόρισμα 3.3.1.5(iii) για κάθε $i > 30 > \frac{1}{2}(4 \cdot 32 - 3 \cdot 23)$ ισχύει $A_i = 0$ ή 3. Οπότε $A_{32} = 0$ ή 3 . Έστω ότι $A_{32} = 3$. τότε από το πόρισμα 3.3.1.5(iv) για $i = 32$ έχουμε ότι $A_j = 0$ για κάθε $j > 128 - 69 - 32 = 27$. Οπότε, $A_{28} = A_{31} = 0$. Η εξίσωση (c) γίνεται

$A_{26} + 2A_{27} = 128.$

Όμως κάθε A_i ($i \neq 0$) είναι πολλαπλάσιο του 3 (αφού τα πολλαπλάσια μιας κωδικής λέξης είναι πάλι κωδικές λέξεις) όμως το 128 δεν διαιρείται με 3, άρα άτοπο. Οπότε αναγκαστικά $A_{32} = 0$. Από το πόρισμα 3.3.1.5(iii) έχουμε ότι $A_{31} = 0$ ή 3. Στην εξίσωση (2.2) αν τα x και y είναι κωδικές λέξεις βάρους τουλάχιστον 28 έχουμε ότι

$$\sum_{i=1}^{3} w(x + iy) \leq 128 - 56 - 4z = 72 - 4z,$$

όπου z συμβολίζει το πλήθος των συντεταγμένων που είναι μηδέν ταυτόχρονα στο x και στο y. Οπότε, επειδή $w(x + iy) \geq 23$ για κάθε i, πρέπει $z = 0$. Αυτό σημαίνει ότι οι γραμμικά ανεξάρτητες κωδικές λέξεις δεν έχουν κοινά μηδενικά. Οπότε υπάρχουν το πολύ 8 προβολικά διακεκριμένες κωδικές λέξεις μήκους 28, και το πολύ 7 αν υπάρχει λέξη με βάρος 31, δηλαδή αν $A_{31} > 0$.

Αν $A_{31} = 0$ η εξίσωση 3(b) – 2(c) μας δίνει την σχέση

$3A_{24} + 3A_{26} = 5A_{28} - 147,$

η οποία είναι αδύνατη επειδή $A_{28} \leq 28$ και οπότε το δεξί μέλος είναι αρνητικό.

Οπότε αναγκαστικά $A_{31} = 3$. Τότε έχουμε $A_{24} \leq 24$ και $A_{24} \leq 21$. Οι μόνες πιθανές λύσεις (έχοντας υπ όψην ότι πρέπει να είναι μη-αρνητικά πολλαπλάσια του 3) είναι αυτές που φαίνονται στον πίνακα 4.

Πίνακας 4

	A_{31}	A_{28}	A_{27}	A_{26}	A_{24}	A_{23}
(1)	3	21	33	0	18	180
(2)	3	21	30	6	12	183
(3)	3	21	27	12	6	186
(4)	3	21	24	18	0	189
(5)	3	12	48	0	3	189

Οι κατανομές (1) και (3) δεν μπορεί να συμβαίνουν διότι τότε από την εξίσωση (d) θα προέκυπτε μη-ακέραια τιμή για το B_3. Στην μεν πρώτη περίπτωση έχουμε $99 + 210 + 210 = 3012 - 6B_2$. Δηλαδή $6B_2 = 2493$. Στην δε δεύτερη περίπτωση $81 + 210 + 210 = 3012 - 6B_2$. Δηλαδή $6B_2 = 2511$. Οι υπόλοιπες περιπτώσεις απορρίπτονται με το ακόλουθο επιχείρημα. Επειδή ο C περιέχει μια λέξη βάρους 31, μπορούμε να υποθέσουμε, χωρίς βλάβη της γενικότητας, ότι ο C έχει γεννήτορα πίνακα της μορφής

$$\left[\begin{array}{ccccc|c} 1 & 1 & \ldots & 1 & & 0 \\ \hline & & & & & 0 \\ & & A & & & \\ & & & & & 0 \\ \hline & & & & & 1 \end{array}\right]$$

Ο πίνακας A είναι ένα 2 × 31 πίνακας. Ας υποθέσουμε ότι ένα διατεταγμένο ζευγάρι στοιχείων εμφανίζεται τρεις φορές σαν στήλη του A, έστω $\begin{bmatrix} a \\ b \end{bmatrix}$. Τότε, στον πίνακα G, αφαιρώντας κατάλληλα πολλαπλάσια της γραμμής 1 από τις γραμμές 2 και 3 ώστε να μηδενίσουμε το εμφανιζόμενο ζευγάρι στον πίνακα A (a και b πολλαπλάσια της γραμμής 1 από τις γραμμές 2 και 3 αντίστοιχα) μπορούμε να υποθέσουμε ότι ο A έχει τρεις μηδενικές στήλες. Αυτό σημαίνει ότι, σβήνοντας αυτές τις τρεις στήλες, ο A παράγει έναν [28, 2, 23]-κώδικα, ο οποίος όμως δεν υπάρχει από το φράγμα του Griesmer ($g_4(2, 23) = \sum_{i=0}^{1} \left\lceil \frac{23}{4^i} \right\rceil = 23 + 6 = 29$). Επομένως, από τα 16 διακεκριμένα διατεταγμένα ζευγάρια στοιχείων του $\mathbf{F}_4$, 15 εμφανίζονται δύο φορές και ένα ακριβώς μια φορά σαν στήλες του πίνακα A. Οπότε ο υποκώδικας C ο οποίος παράγεται από τις πρώτες τρεις γραμμές του G είναι μοναδικός, μέχρι ισοδυναμίας, και έχει κατανομή βαρών $A_{23} = 45$, $A_{24} = 15$, $A_{31} = 3$. Αλλά $A_{24} \leq 12$ για όλο των κώδικα C με κατανομή βαρών (2), (4) ή (5). Αυτό μας οδηγεί στο συμπέρασμα ότι δεν υπάρχει $[32, 4, 23]_4$-κώδικας.

Θεώρημα 3.3.2.10 $n_4(4, 25) > 35$ και $n_4(4, 29) > 40$.

Απόδειξη Αν υπήρχε ένας $[35, 4, 25]_4$ ή ένας $[40, 4, 29]_4$-κώδικας τότε, από το πόρισμα 3.3.1.10, θα υπήρχε ένας $[10, 3, 7]_4$ ή ένας $[11, 3, 8]_4$-κώδικας αντίστοιχα. Σε κάθε περίπτωση αυτό έρχεται σε αντίθεση με τον πίνακα 1.

Θεώρημα 3.3.2.11 $n_4(4, 39) > 53$.

Απόδειξη Έστω ότι υπάρχει ένας $[53, 4, 39]_4$-κώδικας. Από το λήμμα 3.3.1.2, έχουμε ότι $B_1 = B_2 = 0$ αφού δεν υπάρχουν $[52, 4, 39]_4$ και $[51, 3, 39]_4$-κώδικες διότι για $[n, 4, 39]_4$ και $[n, 3, 39]_4$-κώδικες το ελάχιστο δυνατό είναι $n = 54$ και 52 αντίστοιχα.

Από το λήμμα 3.3.1.9, $A_i = 0$ για κάθε $i \in \{41, 42, 43, 45, 46, 49, 50, 51\}$. Οι ταυτότητες MacWilliams γίνονται μετά από αναγωγή ομοίων όρων,

(a) $A_{39} + A_{40} + A_{44} + A_{47} + A_{48} + A_{52} + A_{53} = 255$,
(b) $A_{40} + 5A_{44} + 8A_{47} + 9A_{48} + 13A_{52} + 14A_{53} = 231$,
(c) $10A_{44} + 28A_{47} + 36A_{48} + 78A_{52} + 91A_{53} = 468$.

Από το πόρισμα 3.3.1.5, έχουμε ότι $A_{53} = 0$ ή 3. Αν $A_{53} = 3$ τότε $A_i = 0$ για κάθε $i > 42$, σε αντίθεση με την ισότητα (c). Οπότε, $A_{53} = 0$. Ομοίως, $A_{52} = 0$.

Επίσης, από το πόρισμα 3.3.1.5, έχουμε ότι $A_{48} = 0$ ή 3. Είναι άμεσο ότι οι μόνες λύσεις των ισοτήτων (a), (c) είναι τα μη αρνητικά πολλαπλάσια του 3:

(1) $A_{48} = 3$, $A_{44} = 36$, $A_{40} = 24$, $A_{39} = 192$, $A_0 = 1$,
(2) $A_{47} = 6$, $A_{44} = 30$, $A_{40} = 33$, $A_{39} = 186$, $A_0 = 1$.

Από το πόρισμα 3.3.1.5(v), οι 64 κωδικές λέξεις βάρους 0, 40, 44 και 48 σχηματίζουν έναν [53, 3, 40]-κώδικα. Από το λήμμα 2.2, παίρνουμε ότι ένας [53, 3, 40]- κώδικας έχει $B_1 = 0$ (καθώς ένας [52, 3, 40]-κώδικας δεν μπορεί να υπάρχει από το φράγμα του Griesmer διότι $g_4(3, 40) = \sum_{i=0}^{2} \left\lceil \frac{40}{4^i} \right\rceil = 40 + 10 + 3 = 43$).
Συνεπώς, αν εφαρμόσουμε τη δεύτερη ταυτότητα του MacWilliams σε αυτόν τον υποκώδικα, τότε δίνει:

$$5A_{48} + 9A_{44} + 13A_{40} = 795,$$

αλλά δεν ικανοποιείται από κανένα από τις παραπάνω κατανομές βαρών.

Θεώρημα 3.3.2.12 $n_4(4, 43) > 58$.

Απόδειξη Έστω ότι υπάρχει ένας $[58, 4, 43]_4$-κώδικας. Από το λήμμα 2.2, έχουμε ότι $B_1 = B_2 = 0$, καθώς δεν υπάρχουν ούτε $[57, 4, 43]_4$-κώδικες αλλά ούτε και $[56, 3, 43]_4$-κώδικες λόγω του φράγματος του Griesmer διότι $g_4(4, 43) = \sum_{i=0}^{3} \left\lceil \frac{43}{4^i} \right\rceil =$
$43 + 11 + 3 + 1 = 58$ και $g_4(3, 43) = \sum_{i=0}^{2} \left\lceil \frac{43}{4^i} \right\rceil = 43 + 11 + 3 = 57$.

Από το λήμμα 3.3.1.9, έχουμε ότι $A_i = 0$ για κάθε $i \in \{45, 46, 47, 48, 49, 50, 51, 53, 54, 55, 56, 57\}$. Οι πρώτες τρεις ταυτότητες του MacWilliams γίνονται μετά από αναγωγή ομοίων όρων ως εξής

$A_{43} + A_{44} + A_{52} + A_{58} = 255$,
$A_{44} + 9A_{52} + 15A_{58} = 171$,
$12A_{52} + 35A_{58} = 138$.

Από το πόρισμα 3.3.1.5, έχουμε ότι $A_{58} = 0$ ή 3. Καθεμιά από αυτές τις περιπτώσεις δίνει μια μη ακέραια τιμή για το A_{52} , οπότε ο κώδικας δεν υπάρχει.

Στο [Gre2] οι P.P. Greenough and R. Hill γράφουν: «Θα ενδιαφερόμασταν να μάθουμε για την επίλυση μερικών από τις υπόλοιπες 10 περιπτώσεις του πίνακα 2. Ενδιαφερόμαστε ιδιαίτερα για την ύπαρξη ή διαφορετικά την κατασκευή ενός [57, 4, 42]-κώδικα, για τον οποίο έχουμε δείξει ότι για τα βάρη των κωδικών λέξεων ενός τέτοιου κώδικα πρέπει να ισχύει:

$$A_0 = 1, A_{42} = 192, A_{44} = 36, A_{48} = 27».$$

Το πρόβλημα για d = 42, και συνολικά για 8 από τις 10 υπόλοιπες περιπτώσεις, λύθηκε τελικά από τον ίδιο τον R. Hill, μαζί με τον I. Landgev [HL], λίγους μήνες αργότερα.

3.3.3 Οι υπόλοιπες δέκα τιμές του $n_4(4, d)$

Στο [HL] μπορείτε να βρείτε την απόδειξη για d = 41, 42, 71, 72, 77, 78, 79 και 80.

Συγκεκριμένα, $n_4(4, 41) = 57$, $n_4(4, 42) = 58$, $n_4(4, 71) = 96$, $n_4(4, 72) = 97$, $n_4(4, 77) = 105$, $n_4(4, 78) = 106$, $n_4(4, 79) = 107$, $n_4(4, 80) = 108$.

Στο [Lan1] μπορείτε να βρείτε την απόδειξη για d = 37 και 38.

Συγκεκριμένα, $n_4(4, 37) = 52$ και $n_4(4, 38) = 53$

Ο ολοκληρωμένος πίνακας για k = 4 έχει ως εξής

Οι τιμές του $n_4(4, d)$

d	$g_4(4, d)$	$n_4(4, d)$	απόκλιση	d	$g_4(4, d)$	$n_4(4, d)$	απόκλιση
1	4	4	0	33	46	46	0
2	5	5	0	34	47	47	0
3	6	7	1	35	48	48	0
4	7	8	1	36	49	49	0
5	9	9	0	37	51	52	1
6	10	10	0	38	52	53	1
7	11	12	1	39	53	54	1
8	12	13	1	40	54	55	1
9	14	14	0	41	56	57	1
10	15	15	0	42	57	58	1
11	16	16	0	43	58	59	1
12	17	17	0	44	59	60	1
13	19	20	1				
14	20	21	1				
15	21	22	1				
16	22	23	1				
17	25	25	0	65	89	89	0
18	26	26	0	66	90	90	0
19	27	27	0	67	91	91	0
20	28	28	0	68	92	92	0
21	30	30	0	69	94	94	0
22	31	31	0	70	95	95	0
23	32	33	1	71	96	96	0
24	33	34	1	72	97	97	0
25	35	36	1	73	99	99	0
26	36	37	1	74	100	100	0
27	37	38	1	75	101	101	0
28	38	39	1	76	102	102	0
29	40	41	1	77	104	105	1
30	41	42	1	78	105	106	1
31	42	43	1	79	106	107	1
32	43	44	1	80	107	108	1

3.3.4 Βέλτιστοι τετραδικοί κώδικες διάστασης 5

Από το φράγμα του Griesmer προκύπτει ότι $n_4(5, d) = g_4(5, d)$ για $d \geq 369$.

Υπάρχουν πολλοί μαθηματικοί που προσπάθησαν να λύσουν το πρόβλημα της εύρεσης του $n_4(5, d)$.

Η σημαντικότερη προσφορά στην επίλυση του προβλήματος έχει γίνει από τον Tatsuya Maruta. Το 2001 (στο [Mar2]) απέδειξε την μη ύπαρξη κωδίικων με παραμέτρους $[400, 5, 299]_4$, $[401, 5, 300]_4$, $[405, 5, 303]_4$, $[406, 5, 304]_4$, $[485, 5, 363]_4$, $[486, 6, 364]_4$ οι οποίοι θα ικανοποιούσαν το φράγμα του Griesmer. Για την απόδειξη έδωσε μια ταξινόμηση των κωδίκων με παραμέτρους $[86, 4, 64]_4$, $[101, 4, 75]_4$, $[102, 4, 76]_4$, $[122, 4, 91]_4$.

Για παράδειγμα, έδειξε ότι ένας $[102, 4, 76]_4$ είναι μοναδικός, μέχρι ισοδυναμίας. Ένας τέτοιος κώδικας προκύπτει από πλέξιμο (concatenation) ενός $[17, 4, 12]_4$-κώδικα με έναν $[85, 4, 64]_4$-κώδικα. Επιπλέον κάθε $[101, 4, 75]_4$ μπορεί να επεκταθεί σε έναν $[102, 4, 76]_4$-κώδικα.

Στο [Lan2] αποδείχθηκε ότι $g_4(5, d) \leq n_4(5, d) \leq g_4(5, d) + 2$ για $d = 299, 300, 303, 304, 363, 364$. Πρόσφατα αποδείχθηκε ότι $n_4(5, d) \leq g_4(5, d) + 1$ για $d = 299, 300, 303, 304, 363, 364$. Οπότε, τώρα γνωρίζουμε ότι για αυτές τις τιμές του d ισχύει $n_4(5, d) \leq g_4(5, d) + 1$.

Οι γνωστές τιμές μέχρι σήμερα υπάρχουν στον πίνακα 5. Ο πίνακας υπάρχει στο διαδίκτυο: http://www.geocities.com/mars39.geo/griesmer.htm και ενημερώνεται κάθε φορά που προκύπτει ένα νέο αποτέλεσμα.

Πίνακας 5 – Τιμές και φράγματα για το $n_4(5, d)$

d	$g_4(5,d)$	$n_4(5,d)$	d	$g_4(5,d)$	$n_4(5,d)$
1	5	5	57	78	79-81
2	6	6	58	79	80-82
3	7	8	59	80	81-83
4	8	9	60	81	82-84
5	10	10	61	83	84-85
6	11	11	62	84	85-86
7	12	13	63	85	87
8	13	14	64	86	88
9	15	16	65	90	90-91
10	16	17	66	91	91-92
11	17	19	67	92	92-93
12	18	20	68	93	93-94
13	20	21	69	95	95-96
14	21	22	70	96	96-97
15	22	23	71	97	98
16	23	24	72	98	99
17	26	27	73	100	101
18	27	28	74	101	102

19	28	29	75	102	103-104
20	29	30	76	103	104-105
21	31	32	77	105	106
22	32	33	78	106	107
23	33	34	79	107	108
24	34	35	80	108	109
25	36	37	81	111	111-112
26	37	38	82	112	112-113
27	38	39	83	113	113-114
28	39	40	84	114	114-115
29	41	42	85	116	117
30	42	43	86	117	118
31	43	44-45	87	118	119
32	44	46	88	119	120
33	47	48	89	121	122-123
34	48	49	90	122	123-124
35	49	50	91	123	124-125
36	50	51	92	124	125-126
37	52	53-54	93	126	127-128
38	53	54-55	94	127	128-129
39	54	55-56	95	128	129-130
40	55	56-57	96	129	130-131
41	57	58-59	97	132	133-134
42	58	59-60	98	133	134-135
43	59	60-61	99	134	135-136
44	60	61-62	100	135	136-137
45	62	63-64	101	137	138
46	63	64-65	102	138	139
47	64	65-66	103	139	140-141
48	65	66-67	104	140	141-142
49	68	69	105	142	143-144
50	69	70	106	143	144-145
51	70	71-72	107	144	145-146
52	71	72-73	108	145	146-147
53	73	74	109	147	148-149
54	74	75	110	148	149-150
55	75	76	111	149	150-151
56	76	77	112	150	151-152
113	153	154-155	169	227	228
114	154	155-156	170	228	229
115	155	156-157	171	229	230
116	156	157-158	172	230	231
117	158	159-160	173	232	233
118	159	160-161	174	233	234
119	160	161-162	175	234	235
120	161	162-163	176	235	236
121	163	164	177	238	239
122	164	165	178	239	240
123	165	166-167	179	240	241
124	166	167-168	180	241	242

125	168	169	181	243	244
126	169	170	182	244	245
127	170	171	183	245	246
128	171	172	184	246	247
129	175	175-176	185	248	249
130	176	176-177	186	249	250
131	177	177-178	187	250	251
132	178	178-179	188	251	252
133	180	180-181	189	253	253
134	181	181-182	190	254	254
135	182	182-183	191	255	255
136	183	183-184	192	256	256
137	185	185-186	193	260	260
138	186	186-187	194	261	261
139	187	188	195	262	262
140	188	189	196	263	263
141	190	191	197	265	265
142	191	192	198	266	266
143	192	193	199	267	267
144	193	194	200	268	268
145	196	197	201	270	270
146	197	198	202	271	271
147	198	199	203	272	272
148	199	200	204	273	273
149	201	202	205	275	276
150	202	203	206	276	277
151	203	204	207	277	278
152	204	205	208	278	279
153	206	207	209	281	281
154	207	208	210	282	282
155	208	209	211	283	283
156	209	210	212	284	284
157	211	212	213	286	286
158	212	213	214	287	287
159	213	214	215	288	289
160	214	215	216	289	290
161	217	218	217	291	292
162	218	219	218	292	293
163	219	220	219	293	294
164	220	221	220	294	295
165	222	223	221	296	297
166	223	224	222	297	298
167	224	225	223	298	299
168	225	226	224	299	300
257	346	346	313	419	420
258	347	347	314	420	421
259	348	348	315	421	422
260	349	349	316	422	423
261	351	351	317	424	425
262	352	352	318	425	426

263	353	353	319	426	427
264	354	354	320	427	428
265	356	356	321	431	431-432
266	357	357	322	432	432-433
267	358	358	323	433	433-434
268	359	359	324	434	434-435
269	361	361	325	436	436-437
270	362	362	326	437	437-438
271	363	363	327	438	438-439
272	364	364	328	439	439-440
273	367	367-368	329	441	441-442
274	368	368-369	330	442	442-443
275	369	369-370	331	443	443-444
276	370	370-371	332	444	444-445
277	372	372-373	333	446	446-447
278	373	373-374	334	447	447-448
279	374	374-375	335	448	448-449
280	375	375-376	336	449	449-450
281	377	377-378	337	452	452-453
282	378	378-379	338	453	453-454
283	379	379-380	339	454	454-455
284	380	380-381	340	455	455-456
285	382	382-383	341	457	457-458
286	383	383-384	342	458	458-459
287	384	384-385	343	459	459-460
288	385	385-386	344	460	460-461
289	388	388-389	345	462	462-463
290	389	389-390	346	463	463-464
291	390	390-391	347	464	465
292	391	391-392	348	465	466
293	393	393-394	349	467	468
294	394	394-395	350	468	469
295	395	395-396	351	469	470
296	396	396-397	352	470	471
297	398	398-400	353	473	473-474
298	399	399-401	354	474	474-475
299	400	401	355	475	476
300	401	402	356	476	477
301	403	403-404	357	478	479
302	404	404-405	358	479	480
303	405	406	359	480	481
304	406	407	360	481	482
305	409	410	361	483	484
306	410	411	362	484	485
307	411	412	363	485	486
308	412	413	364	486	487
309	414	415	365	488	489
310	415	416	366	489	490
311	416	417	367	490	491
312	417	418	368	491	492

Κεφάλαιο 4

Αποκωδικοποίηση κωδίκων με τη χρήση βάσεων Gröbner

4.1 Εισαγωγή

Διαβάζοντας τα προηγούμενα κεφάλαια ο αναγνώστης μπορεί να έβγαλε το συμπέρασμα ότι η θεωρία κωδικοποιήσης είναι ισοδύναμη με την θεωρία της πεπερασμένης γεωμετρίας. Αυτό από πρακτική άποψη δεν είναι αλήθεια. Ένας κώδικας είναι άχρηστος χωρίς έναν αλγόριθμο αποκωδικοποίησης. Για τους μηχανικούς η πλήρης, σωστή και γρήγορη λειτουργία της διαδικασίας κωδικοποίησης και αποκωδικοποίησης είναι σημαντική.

Θα δώσουμε μια μέθοδο αποκωδικοποίησης κυκλικών κωδίκων όπου το σύστημα των εξισώσεων των συνδρόμων μπορεί να λυθεί επακριβώς με βάσεις Gröbner. Την μέθοδο αυτή στη συνέχεια θα τη γενικεύσουμε για όλους τους γραμμικούς κώδικες. Αν και ο αλγόριθμος διορθώνει το πολύ $\left[\frac{d-1}{2}\right]$ λάθη, όπου d η ελάχιστη απόσταση του κώδικα, η πολυπλοκότητα του δεν είναι πολυωνυμική. Αυτό οφείλεται στο γεγονός ότι δεν υπάρχει αλγόριθμος που να υπολογίζει βάσεις Gröbner σε πολυωνυμικό χρόνο. Οι αλγόριθμοι του Ευκλείδη και Sugiyama και των Berlkamp-Massey μας δίνουν έναν ικανοποιητικό τρόπο να αποκωδικοποιήσουμε κυκλικούς κώδικες λύνοντας την εξίσωση κλειδί.

4.2 Στοιχεία της Θεωρίας των Βάσεων Gröbner

Έστω K ένα σώμα. Με $K[X_1, ..., X_n]$ θα συμβολίζουμε τον δακτύλιο των πολυωνύμων με μεταβλητές $X_1, ..., X_n$ και συντελεστές από το σώμα K.

Ταξινόμηση μονωνύμων στο $K[X_1, \ldots, X_n]$

Αρχικά θα χρειαστεί να ορίσουμε ένα είδος ταξινόμησης των μονωνυμικών όρων ενός πολυωνύμου. Για παράδειγμα για να εκτελέσουμε τη διαίρεση δυο πολυωνύμων στο K[X] πρέπει να γράψουμε τους μονωνυμικούς όρους τους σε φθίνουσα σειρά με βάση τη δύναμη του X που περιέχει κάθε όρος. Αντίστοιχα για την απαλοιφή του Gauss πρέπει να τοποθετήσουμε τους συντελεστές των αγνώστων σε ένα πίνακα επομένως χρειάζεται να γνωρίζουμε ποιον όρο θα βάλουμε πρώτο, ποιόν δεύτερο, κλπ.

Παρατηρούμε, ότι μπορούμε να αντιστοιχίσουμε κάθε μονώνυμο του $K[\underline{X}] := K[X_1, \ldots, X_n]$ με μοναδικό τρόπο σε μια διατεταγμένη n-άδα του $\mathbf{Z}_{\geq 0}^n$ ως εξής:

$$X^{\alpha} = X_1^{\alpha_1} X_2^{\alpha_2} \ldots X_n^{\alpha_n} \leftrightarrow \alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n).$$

Ορισμός 4.2.1 Μια **μονωνυμική ταξινόμηση** του $K[X_1, \ldots, X_n]$ είναι μια σχέση $>$ στο $\mathbf{Z}_{\geq 0}^n$, ή ισοδύναμα στο σύνολο των μονωνύμων X^α, $\alpha \in \mathbf{Z}_{\geq 0}^n$ η οποία ικανοποιεί τα εξής:

(i) Η $>$ είναι ολική (ή γραμμική) ταξινόμηση του $\mathbf{Z}_{\geq 0}^n$. Δηλαδή αν $\alpha, \beta \in \mathbf{Z}_{\geq 0}^n$ ισχύει ακριβώς ένα από τα εξής $\alpha > \beta$ ή $\beta > \alpha$ ή $\alpha = \beta$.

(ii) Αν $\alpha, \beta, \gamma \in \mathbf{Z}_{\geq 0}^n$ με $\alpha > \beta$ τότε $\alpha + \gamma > \beta + \gamma$

(iii) Η $>$ είναι **καλή ταξινόμηση** δηλαδή κάθε μη-κενό υποσύνολο του $\mathbf{Z}_{\geq 0}^n$ έχει ελάχιστο στοιχείο ως προς την $>$.

Αναφέρουμε το παρακάτω

Λήμμα 4.2.2 Μια σχέση ταξινόμησης $>$ είναι καλή αν και μόνο αν κάθε γνησίως φθίνουσα ακολουθία του $\mathbf{Z}_{\geq 0}^n$

$$\alpha(1) > \alpha(2) > \alpha(3) > \ldots$$

τελικά τερματίζει.

Στη συνέχεια θα δώσουμε κάποιους ορισμούς μονωνυμικών ταξινομήσεων

Ορισμός 4.2.3 (Λεξικογραφική ταξινόμηση) Έστω $\alpha = (\alpha_1, \ldots, \alpha_n)$ και $\beta = (\beta_1, \ldots, \beta_n)$ στοιχεία του $\mathbf{Z}_{\geq 0}^n$. Θα λέμε ότι $\alpha >_{lex} \beta$ αν στο διάνυσμα $\alpha - \beta \in \mathbf{Z}^n$, το πρώτο από τα αριστερά μη-μηδενικό στοιχείο είναι θετικό. Θα γράφουμε $X^\alpha >_{lex} X^\beta$ αν $\alpha >_{lex} \beta$.

Παραδείγματα 4.2.4

a. $(1, 2, 0) >_{lex} (0, 3, 4)$ αφού $(1, 2, 0) - (0, 3, 4) = (1, -1, -4)$.
b. $(3, 2, 4) >_{lex} (3, 2, 1)$ αφού $(3, 2, 4) - (3, 2, 1) = (0, 0, 3)$.
c. Οι μεταβλητές $X_1, X_2, \ldots, X_n$ ταξινομούνται φυσιολογικά με την λεξικογραφική ταξινόμηση

$$(1, 0, \ldots, 0) >_{lex} (0, 1, 0, \ldots, 0) >_{lex} \ldots >_{lex} (0, \ldots, 0, 1)$$

επομένως $X_1 >_{lex} X_2 >_{lex} \ldots >_{lex} X_n$.

Ορισμός 4.2.5 (Βαθμωτή Λεξικογραφική ταξινόμηση) Έστω $\alpha = (\alpha_1, \ldots, \alpha_n)$ και $\beta = (\beta_1, \ldots, \beta_n)$ στοιχεία του $\mathbf{Z}_{\geq 0}^n$. Θα λέμε ότι $\alpha >_{grlex} \beta$ αν $|\alpha| > |\beta|$ είτε $|\alpha| = |\beta|$ και $\alpha >_{lex} \beta$. Όπου $|\alpha| = \sum_{i=1}^n \alpha_i$ και $|\beta| = \sum_{i=1}^n \beta_i$

Παραδείγματα 4.2.6

a. $(1, 2, 3) >_{grlex} (3, 2, 0)$ αφού $|(1, 2, 3)| = 6 > |(3, 2, 0)| = 5$.

b. $(1, 2, 4) >_{grlex} (1, 1, 5)$ αφού $|(1, 2, 4)| = 7 = |(1, 1, 5)|$ και $(1, 2, 4) >_{lex} (1, 1, 5)$.
c. Οι μεταβλητές $X_1, X_2, \ldots, X_n$ ταξινομούνται με βάση την λεξικογραφική ταξινόμηση.

Ορισμός 4.2.7 (Βαθμωτή Αντίστροφη Λεξικογραφική ταξινόμηση) Έστω α και β στοιχεία του $\mathbf{Z}^n_{\geq 0}$. Θα λέμε ότι $\alpha >_{grevlex} \beta$ αν $|\alpha| > |\beta|$ είτε $|\alpha| = |\beta|$ και στο διάνυσμα $\alpha - \beta \in \mathbf{Z}^n$, το πρώτο από τα δεξιά μη-μηδενικό στοιχείο είναι αρνητικό.

Παραδείγματα 4.2.8

a. $(4, 7, 1) >_{grevlex} (4, 2, 3)$ αφού $|(4, 7, 1)| > |(4, 2, 3)| = 9$.
b. $(1, 5, 2) >_{grevlex} (4, 1, 3)$ αφού $|(1, 5, 2)| = 8 = |(4, 1, 3)|$ και $(1, 5, 2) – (4, 1, 3) = (–3, 4, –1)$.
c. Οι μεταβλητές $X_1, X_2, \ldots, X_n$ ταξινομούνται φυσιολογικά όπως και στην λεξικογραφική ταξινόμηση.

Ας πάρουμε το πολυώνυμο $f = 4XY^2Z + 4Z^2 – 5X^3 + 7X^2Z^2 \in K[X, Y, Z]$. Θα το ταξινομήσουμε με τους τρεις τρόπους ταξινόμησης που αναφέραμε παραπάνω. Θα θεωρήσουμε $X > Y > Z$.

a. Με την λεξικογραφική ταξινόμηση

$$f = – 5X^3 + 7X^2Z^2 + 4XY^2Z + 4Z^2$$

b. Με την βαθμωτή λεξικογραφική ταξινόμηση

$$f = 7X^2Z^2 + 4XY^2Z – 5X^3 + 4Z^2$$

c. Με την βαθμωτή αντίστροφη λεξικογραφική ταξινόμηση

$$f = 4XY^2Z + 7X^2Z^2 – 5X^3 + 4Z^2$$

Στη συνέχεια θα χρησιμοποιήσουμε την παρακάτω ορολογία

Ορισμοί 4.2.9 Έστω $f = \sum_\alpha \lambda_\alpha x^\alpha$ ένα μη-μηδενικό πολυώνυμο του $K[X_1, \ldots, X_n]$ και έστω > μια μονωνυμική ταξινόμηση.

(i) Ο **πολυβαθμός** (multideg) του f είναι

$$\text{multideg}(f) = \max\{\alpha \in \mathbf{Z}^n_{\geq 0} : \lambda_\alpha \neq 0\}$$

(ii) Η **οδηγός συντεταγμένη** (leading coefficient) του f είναι

$$LC(f) = \lambda_{\text{multideg}(f)} \in K$$

(iii) Το **οδηγό μονώνυμο** (leading monomial) του f είναι

$$LM(f) = X^{\text{multideg}(f)}$$

(iv) Ο **οδηγός όρος** (leading term) του f είναι

$$LT(f) = LC(f) \cdot LM(f)$$

Για παράδειγμα, αν $f = 4XY^2Z + 4Z^2 – 5X^3 + 7X^2Z^2 \in K[X, Y, Z]$ όπως και πριν και με > συμβολίσουμε την λεξικογραφική ταξινόμηση τότε

$$multideg(f) = (3, 0, 0)$$
$$LC(f) = –5$$
$$LM(f) = X^3$$
$$LT(f) = –5\ X^3$$

Ο πολυβαθμός του f έχει τις ακόλουθες χρήσιμες ιδιότητες

Λήμμα 4.2.10 Έστω $f, g \in K[X_1, …, X_n]$ δυο μη-μηδενικά πολυώνυμα. Τότε:

(i) $multideg(fg) = multideg(f) + multideg(g)$.
(ii) Αν $f + g \neq 0$ τότε $multideg(f + g) \leq \max\{multideg(f), multideg(f)\}$. Αν, επιπλέον, ισχύει $multideg(f) \neq multideg(g)$ τότε στην παραπάνω σχέση ισχύει η ταυτότητα.

Μονωνυμικά ιδεώδη και το λήμμα του Dickson

Σε αυτή την ενότητα θα μελετήσουμε το πρόβλημα της περιγραφής ενός ιδεώδους για μονωνυμικά ιδεώδη. Θα ξεκινήσουμε ορίζοντάς τα στο $K[X_1, …, X_n]$.

Ορισμός 4.2.11 Ένα ιδεώδες I του $K[X_1, …, X_n]$ θα λέγεται **μονωνυμικό** αν υπάρχει υποσύνολο A του $\mathbf{Z}_{\geq 0}^n$ (μπορεί και άπειρο) τέτοιο ώστε το I να αποτελείται από όλα τα πολυώνυμα τα οποία είναι πεπερασμένα αθροίσματα της μορφής $\sum_{\alpha \in A} h_\alpha X^\alpha$,όπου $h_\alpha \in K[X_1, …, X_n]$. Τότε γράφουμε $I = \langle X^\alpha : \alpha \in A \rangle$.

Για παράδειγμα το $I = \langle X^4Y^2, X^3Y^4, X^2Y^5 \rangle$ είναι μονωνυμικό ιδεώδες του K[X, Y].

Στη συνέχεια θα χαρακτηρίσουμε όλα τα μονώνυμα τα οποία βρίσκονται σε ένα μονωνυμικό ιδεώδες.

Λήμμα 4.2.12 Έστω $I = \langle X^\alpha : \alpha \in A \rangle$ ένα μονωνυμικό ιδεώδες. Το μονώνυμο X^β ανήκει στο I αν και μόνο αν το X^β διαιρείται από το X^α για κάποιο $\alpha \in A$.

Από αυτό το λήμμα προκύπτει και το επόμενο.

Λήμμα 4.2.13 Έστω I ένα μονωνυμικό ιδεώδες και έστω $f \in K[X_1, …, X_n]$. Τότε οι ακόλουθες προτάσεις είναι ισοδύναμες:

(i) $f \in I$.
(ii) Κάθε όρος του f ανήκει στο I.
(iii) Το f είναι K-γραμμικός συνδυασμός μονωνύμων του I.

Σαν άμεση συνέπεια του (iii) του λήμματος 4.2.12 είναι το γεγονός ότι κάθε μονωνυμικό ιδεώδες ορίζεται μονοσήμαντα από τα μονώνυμα που περιέχει. Επομένως, προκύπτει η ακόλουθη πρόταση.

Πρόταση 4.2.14 Δύο μονωνυμικά ιδεώδη ταυτίζονται αν και μόνο αν περιέχουν τα ίδια μονώνυμα.

Το βασικό αποτέλεσμα αυτής της ενότητας είναι ότι όλα τα μονωνυμικά ιδεώδη του $K[X_1, \ldots, X_n]$ είναι πεπερασμένα παραγόμενα.

Θεώρημα 4.2.15 (Λήμμα του Dickson) Ένα μονωνυμικό ιδεώδες $I = \langle X^\alpha : \alpha \in A \rangle$ του $K[X_1, \ldots, X_n]$ μπορεί να γραφεί στη μορφή

$$I = \langle X^{\alpha(1)}, \ldots, X^{\alpha(s)} \rangle,$$

όπου $\alpha(1), \ldots, \alpha(s) \in A$. Πιο συγκεκριμένα το I έχει πεπερασμένη βάση.

Η απόδειξη του θεωρήματος γίνεται με επαγωγή ως προς τον αριθμό των μεταβλητών. Μπορούμε να χρησιμοποιήσουμε το λήμμα του Dickson για να αποδείξουμε την παρακάτω

Πρόταση 4.2.16 Έστω $>$ μια σχέση στο $\mathbf{Z}_{\geq 0}^n$ η οποία ικανοποιεί τις παρακάτω προτάσεις:

(i) Η $>$ είναι ολική (ή γραμμική) ταξινόμηση του $\mathbf{Z}_{\geq 0}^n$. Δηλαδή αν $\alpha, \beta \in \mathbf{Z}_{\geq 0}^n$ ισχύει ακριβώς ένα από τα εξής $\alpha > \beta$ ή $\beta > \alpha$ ή $\alpha = \beta$.

(ii) Αν $\alpha, \beta, \gamma \in \mathbf{Z}_{\geq 0}^n$ με $\alpha > \beta$ τότε $\alpha + \gamma > \beta + \gamma$

Τότε η $>$ είναι καλή ταξινόμηση αν και μόνο αν $\alpha \geq 0$ για κάθε $\alpha \in \mathbf{Z}_{\geq 0}^n$.

Άμεσο αποτέλεσμα της πρότασης 4.2.16 είναι η απλοποίηση του ορισμού της μονωνυμικής ταξινόμησης με την αντικατάσταση της συνθήκης (iii) με την ισοδύναμή της. Με αυτό τον τρόπο μπορούμε να εξετάζουμε πολύ πιο εύκολα αν μια ταξινόμηση είναι μονωνυμική ταξινόμηση.

Το θεώρημα βάσης του Hilbert και βάσεις Gröbner

Από τη στιγμή που έχουμε ορίζει μια μονωνυμική ταξινόμηση κάθε πολυώνυμο του $K[X_1, \ldots, X_n]$ έχει μοναδικό οδηγό όρο. Επομένως, για κάθε ιδεώδες I, μπορούμε να ορίσουμε το ιδεώδες των οδηγών όρων του ως εξής:

Ορισμός 4.2.17 Έστω I ένα μη-μηδενικό ιδεώδες του $K[X_1, \ldots, X_n]$.

(i) Θα συμβολίζουμε με LT(I) το σύνολο των οδηγών όρων του I. Με άλλα λόγια

$$LT(I) = \{cX^\alpha : \text{υπάρχει } f \in I \text{ με } LT(f) = cX^\alpha\}$$

(ii) Θα συμβολίζουμε με $\langle LT(I) \rangle$ το ιδεώδες που παράγεται από τα στοιχεία του LT(I).

Ας πάρουμε $I = \langle f_1, f_2, \ldots, f_s \rangle$. Τότε θα θέλαμε τα ιδεώδη $\langle LT(f_1), LT(f_2), \ldots, LT(f_s) \rangle$ και $\langle LT(I) \rangle$ να ταυτίζονται. Από τον ορισμό επειδή $f_1, f_2, \ldots, f_s \in I$ έχουμε ότι $LT(f_1), LT(f_2), \ldots, LT(f_s) \in LT(I)$ και επομένως

$$\langle LT(f_1), LT(f_2), \ldots, LT(f_s) \rangle \subseteq \langle LT(I) \rangle.$$

Ωστόσο η ισότητα δεν ισχύει πάντοτε. Αυτό φαίνεται από το ακόλουθο παράδειγμα.

Παράδειγμα 4.2.18 Έστω $I = \langle f_1, f_2 \rangle$ όπου $f_1 = X^3 - 2XY$ και $f_2 = X^2Y - 2Y^2 + X$. Θα χρησιμοποιήσουμε την βαθμωτή λεξικογραφική ταξινόμηση στο $K[X, Y]$. Ισχύει

$$X(X^2Y - 2Y^2 + X) - Y(X^3 - 2XY) = X^2$$

επομένως $X^2 \in I$. Επομένως $X^2 = LT(X^2) \in LT(I)$. Ωστόσο το X^2 δεν διαιρείται ούτε από το $LT(f_1) = X^3$ ούτε από το $LT(f_2) = X^2Y$ επομένως δεν ανήκει στο μονωνυμικό ιδεώδες $\langle LT(f_1), LT(f_2) \rangle$. (Βλ. λήμμα 4.2.12)

Πρόταση 4.2.19 Έστω I ιδεώδες του $K[X_1, \ldots, X_n]$.

(i) Το $\langle LT(I) \rangle$ είναι μονωνυμικό ιδεώδες.
(ii) Υπάρχουν $g_1, \ldots, g_t \in I$ τέτοια ώστε $\langle LT(I) \rangle = \langle LT(g_1), \ldots, LT(g_t) \rangle$.

Απόδειξη (i) Το οδηγά μονώνυμα $LM(g)$ των πολυωνύμων $g \in I - \{0\}$ παράγουν το μονωνυμικό ιδεώδες $\langle LM(g) : g \in I - \{0\} \rangle$. Επειδή τα $LM(g)$ και $LT(g)$ διαφέρουν μόνο κατά μη-μηδενική σταθερά έχουμε ότι

$$\langle LM(g) : g \in I - \{0\} \rangle = \langle LT(g) : g \in I - \{0\} \rangle.$$

Αποδεικνύεται ότι $\langle LT(g) : g \in I - \{0\} \rangle = \langle LT(I) \rangle$. Δηλαδή, $\langle LT(I) \rangle = \langle LM(g) : g \in I - \{0\} \rangle$ και επομένως το $\langle LT(I) \rangle$ είναι μονωνυμικό ιδεώδες.

(ii) Επειδή $\langle LT(I) \rangle$ παράγεται από τα μονώνυμα $LM(g)$ για $g \in I - \{0\}$ το λήμμα του Dickson μας λεει ότι $\langle LT(I) \rangle = \langle LM(g_1), \ldots, LM(g_t) \rangle$ για πεπερασμένα σε πλήθος πολυώνυμα $g_1, \ldots, g_t \in I$. Επειδή τα $LM(g_i)$ διαφέρουν από τα $LT(g_i)$ κατά μια μη-μηδενική σταθερά έπεται ότι $\langle LT(I) \rangle = \langle LT(g_1), \ldots, LT(g_t) \rangle$ το οποίο ολοκληρώνει την απόδειξη.

Μπορούμε τώρα να χρησιμοποιήσουμε την πρόταση 4.2.19 και τον αλγόριθμο διαίρεσης για να αποδείξουμε ότι κάθε πολυωνυμικό ιδεώδες είναι πεπερασμένα παραγόμενο, δίνοντας έτσι θετική απάντηση στο πρόβλημα της περιγραφής ενός ιδεώδους. Έστω I ιδεώδες του $K[X_1, \ldots, X_n]$ και ας θεωρήσουμε το αντίστοιχο ιδεώδες $\langle LT(I) \rangle$. Επιλέγουμε μια μονωνυμική ταξινόμηση την οποία θα χρησιμοποιήσουμε στον αλγόριθμο διαίρεσης και στον υπολογισμό των οδηγών όρων.

Θεώρημα 4.2.20 (Θεώρημα βάσης του Hilbert) Κάθε ιδεώδες I του $K[X_1, \ldots, X_n]$ είναι πεπερασμένα παραγόμενο. Δηλαδή, υπάρχουν πολυώνυμα $g_1, \ldots, g_t \in I$ τέτοια ώστε $I = \langle g_1, \ldots, g_t \rangle$.

Απόδειξη Αν $I = \{0\}$ το θεώρημα ισχύει. Αν $I \neq \{0\}$ τότε περιέχει κάποιο μη-μηδενικό πολυώνυμο. Τότε ένα σύνολο από πολυώνυμα του I που να το παράγουν μπορεί να δημιουργηθεί ως εξής: Από την πρόταση 3 (ii) υπάρχουν $g_1, \ldots, g_t \in I$ τέτοια ώστε $\langle LT(I) \rangle = \langle LT(g_1), \ldots, LT(g_t) \rangle$. Ισχυριζόμαστε ότι $I = \langle g_1, \ldots, g_t \rangle$.

Αρχικά παρατηρούμε ότι $\langle g_1, \ldots, g_t \rangle \subseteq I$, αφού $g_1, \ldots, g_t \in I$. Αρκεί να δείξουμε ότι $I \subseteq \langle g_1, \ldots, g_t \rangle$. Έστω ένα πολυώνυμο $f \in I$. Εφαρμόζουμε τον αλγόριθμο διαίρεσης διαιρώντας το f με τα $g_1, \ldots, g_t$ και παίρνουμε μια έκφραση της μορφής

$$f = \alpha_1 g_1 + \ldots + \alpha_t g_t + r$$

όπου κάθε όρος του r δεν διαιρείται με κανένα από τα $LT(g_1), \ldots, LT(g_t)$. Αν δείξουμε ότι $r = 0$ θα έχουμε τελειώσει. Παρατηρούμε ότι

$$r = f - \alpha_1 g_1 + \ldots + \alpha_t g_t \in I.$$

Αν $r \neq 0$ τότε $LT(r) \in \langle LT(I) \rangle = \langle LT(g_1), \ldots, LT(g_t) \rangle$ και από το λήμμα 4.2.12 αυτό έπεται ότι το LT(r) διαιρείται από κάποιο $LT(g_i)$ το οποίο είναι άτοπο από τον τρόπο που έχουμε ορίσει το υπόλοιπο. Επομένως, $r = 0$. Οπότε

$$f = \alpha_1 g_1 + \ldots + \alpha_t g_t \in \langle g_1, \ldots, g_t \rangle$$

και η απόδειξη ολοκληρώθηκε.

Η βάση $\langle g_1, \ldots, g_t \rangle$ την οποία διαλέξαμε στο θεώρημα για να λύσουμε το πρόβλημα της περιγραφής ενός ιδεώδους I είχε την παραπάνω ιδιότητα $\langle LT(I) \rangle = \langle LT(g_1), \ldots, LT(g_t) \rangle$. Έχουμε δει ότι αυτό δεν ισχύει για όλες τις βάσεις ενός ιδεώδους. Θα δώσουμε στις βάσεις που ικανοποιούν αυτή την συνθήκη το παρακάτω όνομα.

Ορισμός 4.2.21 Σταθεροποιούμε μια μονωνυμική ταξινόμηση. Ένα πεπερασμένο υποσύνολο $G = \{g_1, \ldots, g_t\}$ ενός ιδεώδους I θα λέγεται **βάση Gröbner** (ή **κανονική βάση**) αν ισχύει

$$\langle LT(I) \rangle = \langle LT(g_1), \ldots, LT(g_t) \rangle.$$

Από την απόδειξη του θεωρήματος 4.2.20 προκύπτει το ακόλουθο αποτέλεσμα

Πρόταση 4.2.22 Σταθεροποιούμε μια μονωνυμική ταξινόμηση. Κάθε μη-μηδενικό ιδεώδες I του $K[X_1, \ldots, X_n]$ έχει βάση Gröbner. Επιπλέον, κάθε βάση Gröbner ενός ιδεώδους I είναι βάση του I.

Απόδειξη Έστω I ένα μη-μηδενικό ιδεώδες του $K[X_1, \ldots, X_n]$. Στην απόδειξη του θεωρήματος βάσης Hilbert δείξαμε ότι πάντα μπορούμε να κατασκευάσουμε ένα σύνολο $G = \{g_1, \ldots, g_t\}$ το οποίο είναι βάση Gröbner. Για το δεύτερο μέρος της πρότασης παρατηρήστε ότι στην απόδειξη του θεωρήματος βάσης Hilbert δείξαμε

ότι αν $<LT(I)> = <LT(g_1), \ldots, LT(g_t)>$ τότε $I = <g_1, \ldots, g_t>$ και επομένως το G είναι βάση του I.

Ας θεωρήσουμε το ιδεώδες $I = <f_1, f_2>$ του δακτυλίου $K[X, Y]$ όπου $f_1 = X^3 - 2XY$ και $f_2 = X^2Y - 2Y^2 + X$. Το σύνολο $\{f_1, f_2\}$ είναι βάση του I αλλά δεν είναι βάση Gröbner με βάση την βαθμωτή λεξικογραφική ταξινόμηση αφού, όπως δείξαμε και στο παράδειγμα 4.2.18, το X^2 δεν ανήκει στο ιδεώδες $<LT(f_1), LT(f_2)>$.

Στη συνέχεια ας θεωρήσουμε το ιδεώδες $J = <g_1, g_2> = <X + Z, Y - Z>$. Ισχυριζόμαστε ότι τα g_1, g_2 σχηματίζουν μια βάση Gröbner του J αν θεωρήσουμε την λεξικογραφική ταξινόμηση στο $\mathbf{R}[X, Y, Z]$. Με άλλα λόγια θα δείξουμε ότι για κάθε μη-μηδενικό στοιχείο f του J το LT(f) βρίσκεται στο ιδεώδες $<LT(g_1), LT(g_2)> = <X, Y>$. Από το λήμμα 4.2.12 μπορούμε ισοδύναμα να δείξουμε ότι το LT(f) διαιρείται είτε με X είτε με Y.

Έστω λοιπόν, ένα μη-μηδενικό πολυώνυμο $f = Ag_1 + Bg_2 \in J$. Υποθέτουμε ότι το LT(f) δεν διαιρείται ούτε από το X ούτε από το Y. Από τον ορισμό της λεξικογραφικής ταξινόμησης αυτό σημαίνει ότι είναι πολυώνυμο του Z. Ωστόσο, επειδή $f \in J$ το f μηδενίζεται στο γραμμικό υπόχωρο $L = V(J) = V(X + Z, Y - Z) \subset \mathbf{R}^3$. Επειδή οι λύσεις στον L παραμετρικοποιούνται ως εξής: $(x, y, z) = (-t, t, t) \in L$, για κάθε πραγματικό αριθμό t το μόνο πολυώνυμο του Z το οποίο μηδενίζεται στον L είναι το μηδενικό πολυώνυμο και καταλήξαμε σε άτοπο. Επομένως, το $\{g_1, g_2\}$ είναι βάση Gröbner του J.

4.3 Αποκωδικοποίηση κυκλικών κωδίκων με τη χρήση βάσεων Gröbner

Έστω C ένας κυκλικός $[n, k, d]_q$-κώδικας με πολυώνυμο-γεννήτορα g(X) και σύνολο ορισμού $J = J(C) = \{j_1, \ldots, j_r\}$.

Έστω $\mathbf{F}_{q'}$ μια επέκταση του $\mathbf{F}_q$ ($q' = q^e$) η οποία περιέχει όλες τις ρίζες του g(X). Έστω $\alpha \in \mathbf{F}_{q'}$ μια πρωταρχική n-ρίζα της μονάδας. Τότε ένας πίνακας ελέγχου ισοτιμίας του C είναι ο

$$H = \begin{bmatrix} 1 & \alpha^{j_1} & \alpha^{2j_1} & \ldots & \alpha^{2j_1} \\ 1 & \alpha^{j_2} & \alpha^{2j_2} & \ldots & \alpha^{2j_2} \\ 1 & \alpha^{j_3} & \alpha^{2j_3} & \ldots & \alpha^{(n-1)j_3} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \alpha^{j_r} & \alpha^{2j_r} & \ldots & \alpha^{(n-1)j_r} \end{bmatrix}.$$

Έστω $e = e(X)$ το διάνυσμα λάθους μιας ληφθείσας λέξης $y = y(X)$. Τότε,

$$s = yH^T = eH^T$$

και επιπλέον

$$s_i = y(\alpha^{j_i}) = e(\alpha^{j_i})$$

είναι το i-στό στοιχείο του διανύσματος s για i = 1, …, r. Μπορούμε μάλιστα να θεωρήσουμε μια επέκταση $\hat{H}$ του πίνακα H η οποία να είναι ένας n × n πίνακας με i-στή γραμμή

$$[1 \qquad \alpha^i \qquad \alpha^{2i} \qquad ... \qquad \alpha^{(n-1)i}]$$

για i = 1, ..., n. Ορίζουμε $\hat{s} = e\,\hat{H}^T$. Το j-οστό στοιχείο του διανύσματος $\hat{s}$ είναι

$$\hat{s}_j = e(\alpha^j) = \sum_{i=0}^{n-1} \alpha^{ij}$$

για j = 1, ..., n. Αν $j \in J(C)$ τότε $\hat{s}_j = e(\alpha^j) = y(\alpha^j)$, οπότε αυτά τα σύνδρομα είναι γνωστά.

Για την υπόλοιπη παράγραφο θα συμβολίζουμε, για λόγους απλότητας, τα $\hat{s}_j$ με s_j. Παρατηρήστε ότι τα αρχικά s_j θα γράφονται τώρα ως s_{j_i} .

Έστω e = e(X) ένα διάνυσμα λάθους με θέσεις λάθους $i_1, i_2, \ldots, i_t$ και τιμές λάθους $e_{i_1}, e_{i_2}, \ldots, e_{i_t}$. Τότε τα γνωστά σύνδρομα είναι

$$s_j = \sum_{m=1}^{t} e_{i_m} (\alpha^{i_m})^j \,,\ j \in J(C).$$

- Θυμίζουμε ότι, $e_j = 0$ για κάθε $j \notin J(C)$.

Θεωρούμε το ακόλουθο σύστημα εξισώσεων στον δακτύλιο $\mathbf{F}_{q'}[X_1, \ldots, X_u, Y_1, ..., Y_u]$:

$$S(s, u) = \begin{cases} \sum_{m=1}^{u} Y_m X_m^j = s_j & \text{για } j \in J \\ Y_m^q = Y_m & \text{για } m = 1,..., u \\ X_m^n = 1 & \text{για } m = 1,..., u \end{cases}.$$

Παρατηρούμε ότι $X_m = \alpha^{i_m}$ και $Y_m = e_{i_m}$ για m = 1, …, t είναι λύση του S(u, t).

Παράδειγμα 4.3.1 Έστω J = {1, 2}. Αν C είναι ένας κυκλικός κώδικας με σύνολο ορισμού το J, τότε η ελάχιστη απόστασή του είναι τουλάχιστον 3 σύμφωνα με το φράγμα για τους BCH κώδικες. Άρα μπορούμε να διορθώσουμε τουλάχιστον 1 λάθος. Οι εξισώσεις

$$\begin{cases} Y_1 X_1 = s_1 \\ Y_1 X_1^2 = s_2 \end{cases}$$

μας δείχνουν ότι, αν υπάρχει ακριβώς ένα λάθος, η θέση λάθους είναι $x_1 = s_2 s_1^{-1}$. Επίσης, αν q = 2 τότε $s_2 = s_1^2$. Οπότε, $x_1 = s_1$.

Χωρίς απόδειξη παραθέτουμε την ακόλουθη πρόταση:

Πρόταση 4.3.2 Έστω ότι κατά τη μετάδοση μιας κωδικής λέξης προέκυψαν t λάθη και $t \leq \frac{1}{2}(d - 1)$. Τότε το σύστημα S(s, u) πάνω από το $\mathbf{F}_{q'}$ δεν έχει λύσεις όταν u < t. Το σύστημα έχει μοναδική λύση (μέχρι μεταθέσεων) -η οποία αντιστοιχεί στο διάνυσμα λάθους με ελάχιστο βάρος το οποίο ικανοποιεί τις εξισώσεις του συνδρόμου- όταν u = t. Τα X_i της λύσης αντιστοιχούν στις θέσεις λάθους και τα Y_i στις αντίστοιχες τιμές λάθους. Τέλος, όταν u > t τότε για κάθε j το σύστημα έχει μια λύση με $X_1 = \alpha^j$.

Το σύστημα S(s, u) που δώσαμε παραπάνω ορίζει ένα ιδεώδες του δακτυλίου $\mathbf{F}_{q'}[X_1, \ldots, X_u, Y_1, ..., Y_u]$. Θα συμβολίζουμε αυτό το ιδεώδες επίσης με S(s, u) για λόγους απλότητας στους συμβολισμούς.

Το σύνολο λύσεων του ιδεώδους μας δίνει το διάνυσμα λάθους που δημιουργήθηκε κατά την μετάδοση. Θα χρησιμοποιήσουμε τεχνικές της θεωρίας των βάσεων Gröbner για να βρούμε το σύνολο λύσεων.

Θα συμβολίζουμε με < την λεξικογραφική διάταξη – την οποία πολλές φορές ονομάζουμε και διάταξη απαλοιφής (elimination order).

Θυμίζουμε ότι ισχύει η ακόλουθη

Πρόταση 4.3.3 Έστω I ένας ιδεώδες του δακτυλίου $K[Z_1, Z_2, \ldots, Z_w]$. Έστω G μια βάση Gröbner του I με βάση την <. Τότε το $G \cap K[Z_1, Z_2, \ldots, Z_i]$ είναι μια βάση Gröbner του $I \cap K[Z_1, Z_2, \ldots, Z_i]$.

Έστω I ένα ιδεώδες του $K[Z_1, Z_2, ..., Z_w]$ με πεπερασμένες το πλήθος ρίζες πάνω από την αλγεβρική κλειστότητα του K που όλες ορίζονται στο K. Έστω V το σύνολο των ριζών του ιδεώδους I στο K^w. Τότε το σύνολο των ριζών του $I \cap K[Z_1, Z_2, \ldots, Z_i]$ είναι η προβολή του V στις πρώτες i συντεταγμένες. Αυτή η παρατήρηση μπορεί να χρησιμοποιηθεί για να πάρουμε επαγωγικά κάθε ανιχνευτή λάθους (error-locator) ως την πρώτη συντεταγμένη μιας λύσης του S(s, u).

Αναφέρουμε την ακόλουθη

Πρόταση 4.3.4 Έστω ότι κατά τη μετάδοση μιας κωδικής λέξης προέκυψαν t λάθη και $t \leq \frac{1}{2}(d - 1)$. Έστω $g(X_1)$ το μονικό πολυώνυμο - γεννήτορας του ιδεώδους $S(s, t) \cap \mathbf{F}_{q'}[X_1]$. Τότε οι ρίζες του g είναι οι ανιχνευτές λάθους.

Πριν δώσουμε τον τελικό αλγόριθμο αποκωδικοποίησης πρέπει να εξετάσουμε ακόμα κάτι. Υποθέσαμε ότι γνωρίζουμε πόσα λάθη θα συμβούν κατά την μετάδοση (το u του συστήματος S(s, u)). Παρατηρήστε ότι είναι πιο χρονοβόρο να λύσουμε το σύστημα S(s, u) για μεγάλο u από ότι για μικρό. Παρατηρήστε ωστόσο ότι γενικά

μια λέξη με πολλά λάθη είναι λιγότερο πιθανό να προκύψει από ότι μια λέξη με λίγα λάθη.

Θεώρημα 4.3.5 Έστω ότι κατά τη μετάδοση μιας κωδικής λέξης προέκυψαν t λάθη και $t \le \frac{1}{2}(d-1)$. Θα συμβολίζουμε με $l(X_1)$ το μονικό πολυώνυμο εύρεσης λάθους, δηλαδή $l(x) = 0$ αν και μόνο αν x είναι ανιχνευτής λάθους. Έστω $S(s, u)$ ιδεώδες στο $\mathbf{F}_{q'}[X_1, \ldots, X_u, Y_1, \ldots, Y_u]$. Έστω $g(X_1)$ το μονικό πολυώνυμο - γεννήτορας του ιδεώδους $S(s, t) \cap \mathbf{F}_{q'}[X_1]$. Τότε

$$g(X_1) = \begin{cases} 1 & \text{αν } u < t \\ l(X_1) & \text{αν } u = t \\ X_1^n - 1 & \text{αν } u > t \end{cases}.$$

Παρατήρηση 4.3.6 Μπορούμε να αντικαταστήσουμε στην πρόταση 4.3.4 και στο θεώρημα 4.3.5 την υπόθεση «$t \le \frac{1}{2}(d-1)$» με την ασθενέστερη «η ληφθείσα λέξη έχει μοναδική πλησιέστερη κωδική λέξη».

Ας δώσουμε τώρα τον αλγόριθμο αποκωδικοποίησης κυκλικών κωδίκων.

Αλγόριθμος

Είσοδος: y

$s := yH^T$

IF $s_j = 0$ για κάθε $j \in J$ THEN δώσε έξοδο y και ΣΤΑΜΑΤΗΣΕ {Δεν προέκυψαν λάθη}

ELSE

```
u := 1
G := {1};
WHILE 1∈ G DO
        S := {}
        FOR j in J DO
                S := S ∪ {∑_{m=1}^{u} Y_m X_m^j − s_j)}
        OD;
        FOR m from 1 to u DO
                S := S ∪ {Y_m^q − Y_m, X_m^n − 1}
        OD;
        G:=Gröbner(S);
        u := u + 1;
OD;
```

{$1 \notin G$ οπότε δεν υπάρχουν λύσεις}
$g(X_1)$:= το μοναδικό στοιχείο του $G \cap \mathbf{F}_{q'}[X_1]$;
IF $\deg(g(X_1)) > u$ THEN output{ΠΟΛΛΑ ΛΑΘΗ}; stop;
ELSE error-locators := {ρίζες του $g(X_1)$}
Βρες το διάνυσμα λάθους e λύνοντας το γραμμικό σύστημα

Εξοδος: y – e.

Ο αλγόριθμος που δίνουμε έχει το πλεονέκτημα ότι γενικεύεται για όλους τους γραμμικούς κώδικες. Έχει όμως και ένα μεγάλο μειονέκτημα, δεν υπάρχει αλγόριθμος πολυωνικού χρόνου ο οποίος να υπολογίζει βάσεις Gröbner. Αυτό έχει ως αποτέλεσμα ο αλγόριθμος να είναι πολύ αργός.

Βιβλιογραφία

[Ali] Ali A.H., Hirschfeld J.W.P. and Kaneta H. (November 1995) **On the size of arcs in projective spaces**, IEEE Trans. Inform. Theory, vol.41, no.6, 1649-1656.

[All] Alltop, W.O. (1976) **Binary codes with improved minimum weights**, IEEE Trans. Inform. Theory, IT22, 241-243.

[As] E.F. Assmus Jr and H.F. Mattson Jr (1972) **On weights in quadratic-residue codes**, Discrete Mathematics **3.**

[Bak] Baker R.D., Bonisoli A., Cossidente A. and Ebert G. (1999) **Mixed partitions of PG(5,q)**, Discrete Math. **208/209**, 23-29. Διαθέσιμο στο διαδίκτυο: http://www.math.udel.edu/~ebert/papers/mparts_sub.ps.

[Bar] Barát János, Edel Yves, Hill R. and Storme L. (2004) **On complete caps in the projective geometries over F_3 II: New improvements**, Journal of Combinatorial Mathematics and Combinatorial Computing **49**, 9-31. Διαθέσιμο στο διαδίκτυο: http://www.mathi.uni-heidelberg.de/~yves/Papers/PG(6,3).html.

[Barl] Barlotti, A. (1955) **Un estensione del theorema di Segre-Kustaanheimo**, Boll. Un. Mat. Otal. **10**, 96-98.

[BE] Bierbrauer, Jürgen and Edel, Yves (1999) **41 is the largest size of a cap in PG(4,4)**, Designs, Codes and Cryptography **16**, 151-160. Διαθέσιμο στο διαδίκτυο: http://www.mathi.uni-heidelberg.de/~yves/Papers/41cap.html.

[BE2] Bierbrauer, Jürgen and Edel, Yves (1999) **Recursive constructions for large caps**, Bulletin of the Belgian Mathematical Society - Simon Stevin **6**, 249-258. Διαθέσιμο στο διαδίκτυο: http://www.mathi.uni-heidelberg.de/~yves/Papers/RCap.html.

[BE3] Bierbrauer, Jürgen and Edel, Yves (2001) **Large caps in small spaces**, Designs, Codes and Cryptography, **23** (2001), 197-212. Διαθέσιμο στο διαδίκτυο: http://www.mathi.uni-heidelberg.de/~yves/Papers/smallCaps.html.

[BE4] Bierbrauer, Jürgen and Edel, Yves (2002) **Bounds on affine caps**, Journal of Combinatorial Design **10**, 111-115. Διαθέσιμο στο διαδίκτυο: http://www.mathi.uni-heidelberg.de/~yves/Papers/ABound.html.

[Bie] Bierbrauer, Jürgen (2004, April 29) **Finite Geometries**, Διδακτικές Σημειώσεις. Βελτιωμένη έκδοση με προσθήκες από σημειώσεις του ίδιου στις 30 Απριλίου 2002. Διαθέσιμες στο διαδίκτυο: http://www.math.mtu.edu/~jbierbra/HOMEZEUGS/finitegeom04.ps.

[Bie2] Bierbrauer, Jürgen (1999, February 8) **MA 576: Introduction to Codes and their Use**, Διδακτικές Σημειώσεις. Διαθέσιμες στο διαδίκτυο: http://www.math.mtu.edu/~jbierbra/HOMEZEUGS/Codecourse.ps

[Boe] de Boer, Mario and Pellikaan, Ruud (1999), **Gröbner bases for error-correcting codes and their decoding,** "Some tapas of computer algebra" (A.M. Cohen, H. Cuypers and H. Sterk eds.), Chap. 10, Gröbner bases for codes, pp. 237-259, Chap. 11, Gröbner bases for decoding, pp. 260-275, Project 7, The Golay codes, pp. 338-347, Springer-Verlag, Berlin. Διαθέσιμο στο διαδίκτυο: http://www.win.tue.nl/~ruudp/publications.html.

[Bos] Bose, R. C. (1947) **Mathematical theory of the symmetrical factorial design**, Sankhya **8**, 107-166.

[Bouk] I. Boukliev, S.M. Dodunekov, T. Helleseth (1997) **On the [162, 8, 80] codes**, IEEE Trans. Inf. Th., Volume 43 Number 6, November 1997, 2055-2057. Διαθέσιμο στο διαδίκτυο: http://www.ii.uib.no/~oyvind/Papers/onesixtwo.ps.

[Bouy] Iliya Bouyukliev, David B. Jaffe and Vesselin Vavrek (July 2000) **The smallest length of eight-dimensional binary linear codes with prescribed minimum distance,** IEEE Trans. Inform. Theory, Vol.46 Num.**4**, p.1539 – 1544. Διαθέσιμο στο διαδίκτυο: http://www.math.unl.edu/~djaffe/papers/eights.html.

[Bram] D.L. Bramwell (1979) **A note on k – 3 caps in three-dimensional Galois space**, Math. Proc. Camb. Phil. Soc. **86,** 21 – 23.

[Br] A.E. Brouwer's data base of bounds for linear codes
http://www.win.tue.nl/~aeb/voorlincod.html.

[Bro] Brouwer Andries, Verhoeff Tom (1993) **An Updated Table of Minimum-Distance Bounds for Binary Linear Codes**, IEEE Transactions on Information Theory **39(2)**, 662-677. Διαθέσιμο στο διαδίκτυο: http://wwwpa.win.tue.nl/wstomv/publications/ updated-min-distance-table.pdf.

[Bru] Bruen, A. A. and Hirschfeld, J. W. P. (1978) **Application of line geometry over finite fields. II. The Hermitian surface**, Geom. Dedicata **7**, 333-353.

[Cald] A.R. Calderbank and W.M. Kantor (1986) **The geometry of two-weight codes**, Bull. London Math Soc. **18,** 97 – 122.

[CK1] Chao J.M. and Kaneta H. (1997) **Classical arcs in P G(r; q) for 11 ≤ q ≤ 19,** Discrete Mathematics **174**, 87-94. (Proceedings of the international conference on Combinatorics '94**,** Rome & Montesilvano, Italy).

[CK2] Chao J.M. and Kaneta H. (2001) **Classical arcs in P G(r; q) for 23 ≤ q ≤ 27**, Discrete Mathematics **226**, Issue 1-3, 377-385.

[Ede] Edel, Yves, Ιστοσελίδα σχετικά με τα caps: http://www.mathi.uni-heidelberg.de/~yves/Matritzen/CAPs/CAPMatIndex.html

[Edg] Edgar Tom (Spring 2004) **Finite Geometries and Linear Codes**, Master Thesis, Department of Mathematics, Fort Collins, Colorado.

[Ca] Casse, L. R. A. (1969) **A solution to Beniamino Segre's 'Problem $I_{r,q}$' for q even**, Atti. Accad. Naz. Lincei Rend. **46**, 13-20.

[Fa] Faina, G. and Pambianco, F. (1998) **On the spectrum of the values k for which a complete k-cap in PG(n, q) exists**, Journal of Geometry **62**, 84-98.

[Far] Farrell, P.G. (1978) **An introduction to anticodes**, CIM Summer School: Algebraic coding theory and applications.

[FV] Fenton, N. E. and Vámos, P. (1982) **Matroid interpretation of maximal k-arcs in projective spaces**, Rend. Mat. (7) **2**, 573-80.

[Ga] Games, R. A. (1983) **The packing problem for projective geometries over GF(3) with dimension greater than five**, J. Comb. Theory, Series A **35**, 126-144.

[Gly] David Glynn (1999) A 126-cap of PG(5, 4) and its corresponding [126,6,88]-code, Utilitas Mathematica **55**, 201-210.

[Gr] J.H. Griesmer (1960) **A bound for error-correcting codes**, IBM Journal of Research and Development, Volume 4, Number 5, 532-542. Διαθέσιμο στο διαδίκτυο: http://domino.research.ibm.com/tchjr/journalindex.nsf/0/65e912369330feeb85256bfa00683dd7?OpenDocument.

[Gre1] P.P. Greenough (1991) **Searching for optimal linear codes**, MSc. Thesis, Univ. of Salford, 1991.

[Gre2] P.P. Greenlough and R. Hill (1994) **Optimal linear codes over GF(4)**, Discrete Mathematics 125, 187 – 199.

[Gul] T.A. Gulliver and V.K. Bhargava (1992) **Some best rate 1/p and rate (p – 1)/p systematic qyasi-cyclic codes over GF(3) and GF(4)**, IEEE Trans. Inform. Theory **38,** 1369 – 1374.

[Helle1] Helleseth, T. and Ytrehus, Ø. (November, 1989) **How to find a [33, 8, 14] code**, Report in Informatics, no. **41**, Department of informatics, University of Bergen, Norway. Διαθέσιμο στο διαδίκτυο: http://www.ii.uib.no/~oyvind/Papers/en33814.ps

[Helle2] Helleseth, T. and Ytrehus, Ø. (May 1990) **There is no binary [25,8,10] code**, IEEE Trans. Inf. Th., 695-696. Διαθέσιμο στο διαδίκτυο: http://www.ii.uib.no/~oyvind/Papers/rep_25_8.ps.

[HS] Helgert, H. J. and Stinaff, R. D. (1973) **Minimum distance bounds for binary linear codes**, IEEE Trans. Info. Theory **19**, 344-356.

[Hil1] Hill, Raymond (1999) **A First Course in Coding Theory**, Oxford University Press. Βελτιωμένη έκδοση με διορθώσεις, αντίστοιχη με αυτή που κυκλοφόρησε το 1986.

[Hil2] Hill, R. (1973) **On the largest size of cap in $S_{5,3}$**, Atti Accad. Naz. Lincei Rendiconti **54**, 378-384.

[Hil3] Hill, R. (1978) **Caps and Codes,** Discrete Math. **22**, 111-137.

[Hil4] Hill, R. (1983) **On Pellegrino's 20 caps in $S_{4,3}$**, Combinatorial Geometries and their Applications (Rome 1981), Ann. Discrete Math. **18**, 443-448.

[Hil5] Hill, R (Cirencester, 1989) **Optimal linear codes** in Cryptographie and coding, II, volume 33, Inst. Math. Appl. Conf. Ser. New Ser., Oxford Univ. Press, New York, 75-104.

[Hil78] R. Hill (1978) **Some results concerning linear codes and (k, 3)-caps in three-dimensional Galois space**, Math. Proc. Camb. Phil. Soc. **84,** 191 – 205.

[Hil92] R. Hill (1992) **Optimal linear codes** in: C. Mitchell. Ed., Proc. 2nd IMA Conf. on Cryptography and Coding (Oxford Univ. Press, Oxford) 75 – 104.

[HLJSB] Hill R., Landjev I., Jones Ch., Storme L. and Barát J. (2000) **On complete caps in the projective geometries over F_3**, Journal of Geometry **67**, 127-144.

[HL] Hill R. & Landgev I. (June 1994) **On the nonexistence of some quaternary codes**, Proc. IMA conf. Finite Fields and their Applications.

[HN1] R. Hill and D.E. Newton (1988) **Some optimal ternary linear codes**, Ars Combin. 25A, 61 – 72.

[HN2] R. Hill and D.E. Newton (1992) **Optimal ternary linear codes**, Desi. Codes Cryptography **2,** 137 – 157.

[Hir1] Hirschfeld, J. W. P. (1983) **Maximum sets in finite projective spaces**, in Surveys in combinatorics, LMS Lecture Note Series **82**, edited by E. K. Lloyd. Cambridge University Press, 55-76.

[Hir2] Hirschfeld, J. W. P. (1998) **Projective geometries over finite fields**, Second Edition, Oxford University Press. (Διαθέσιμο από την βιβλιοθήκη του Παν. Κρήτης κωδικός: QA471.H58 1998). Δεύτερη έκδοση από βιβλίο που κυκλοφόρησε το 1979. (Διαθέσιμο από την βιβλιοθήκη του Παν. Κρήτης κωδικός: QA471.H58).

[Hir3] Hirschfeld, J.W. P. and Storme, L. (1998) **The packing problem in statistics, coding theory, and finite projective spaces**, J. Statist. Planning Inference **72**, 355-380.

[Hir4] Hirschfeld, J. W. P. and Storme, L. (2000) T**he packing problem in statistics, coding theory, and finite projective spaces: update 2001,** in: A. Blokhuis, J.W.P. Hirschfeld, D. Jungnickel, J.A. Thas (Eds.), Developments in Mathematics, Vol. 3, Finite Geometries, Proceedings of the Fourth Isle of Thorns Conference, Kluwer Academic Publishers, Dordrech, pp. 201-246.

[Ju] Jurick, R.R. (1968) **An algorithm for determining the largest maximally independent set of vectors from an r-dimensional space over a Galois field of n elements**, Tech Rep. AS-TR-68-40, Air Force Systems Command, Wright-Patterson Air Force Base, Ohio.

[Lan1] I. Landgev, T. Maruta, R. Hill (1996) **On the nonexistence of quaternary [51,4,37] codes**, Finite Fields Appl. **2,** 96-110.

[Lan2] Landjev, I. N. and Maruta, T (1999) On the minimum length of quaternary linear codes of dimension five, Discrete Math 202, 145 – 161.

[Log] Logačev, V.W. (1974) **An improvement of the Griemser bound in the case of small code distances**, Optimization methods and their applications (All-Union Summer Seminar, Khakusy, Lake Baikal, 1972), 107 – 111, 182 Silbirsk. Energetic. Inst.. Sibirsk..Otdel. Akad.. nauk SSSR, Irkutsk.

[Mag] Μαγιολαδίτης, Μάριος (2001) **Αλγεβρικές καμπύλες, εικασία του Riemann και κωδικοποίηση**, Διπλωματική Εργασία,, Πανεπιστήμιο Κρήτης. Διαθέσιμη στο διαδίκτυο: http://www.math.uoc.gr/~marios/ergasia.htm.

[Mar2] Maruta, Tatsuya (2001) **On the nonexistentence of some quaternary linear codes of dimension 5**, Discrete Mathematics **238**, 99 – 113.

[MaS] Maneri, C. and Silverman, R. (1966) **A vector space packing problem**, Journal of Algebra **4**, 321-330.

[Me] Meshulam, R. (1995) **On subsets of finite abelian groups with no 3-term arithmetic progression**, Journal of Combin. Theory, Ser. A 71, 168-172.

[MS] Mac-Williams, F.J. and Sloane N.J.A. (1983, 2nd reprint) **The Theory of Error-Correcting Codes**, North-Holland Mathematical Library.

[Lid] Rudolf Lidl - Gunter Pilz (1998) **Applied Abstract Algebra**, Springer-Verlag.

[Liz] Lizak, Pawel (1995, November) **Optimal quaternary linear codes**, Διδακτορική διατριβή, University of Salford.

[Pan] Panella, Gianfranco **Caratterizzazione delle quadriche di uno spazio (tridimensionale) lineare sopra un corpo finito**, Boll. Un. Mat. Ital. (3) **10**, 507-513, 1955.

[Pe] Pellegrino, G. (1970) **Sul massimo ordine delle calotte in $S_{4,3}$**, Matematiche (Catania) **25**, 1-9. Δημοσιεύτηκε επίσης στο Mathematiche **25**, 1971, 149-157.

[Qv] Qvist, B. (1952) **Some remarks concerning curves of the second degree in a finite plane**, Ann. Acad. Sci. Fenn., Ser.A, no. **134**, 1952.

[Se1] Segre, Beniaino (1954) **Sulle ovalli nei plani lineari finiti**, Atti Accad. Naz. Lincei Rendiconti **17**, 1-2.

[Se2] Segre, Beniamino (1955) **Ovals in a finite projective plane**, Canad. J. Math. **7**, 414-416. Μετάφραση στα αγγλικά του [Se1].

[Se3] Segre B. (1955) **Curve razionali normali e k-archi negli spazi finiti**, Ann. Mat. Pura Appl. **39**, 357-79.

[S-S] G. Solomon and J.J.Stiffer (1965, April) **Algebraically punctured cyclic codes**, Information and Control, Volume 8, no. **2**, 170-179.

[Ta] Tallini, G. (1964) **Calotte complete di $S_{4,q}$ contenenti due quadriche ellittiche quali sezioni iperpiane**, Rend.Mat e Appl. **23**, 108-123.

[Til1] van Tilborg, H.C.A (1978) **On quasi-cyclic codes with rate 1/m**, IEEE Trans. Inform. Theory, IT-24, 628-630.

[Til2] van Tilborg, H.C.A (1980) **On the uniqueness resp. nonexistence of certain codes meeting the Griesmer bound**, Inform. And Control **44**, 16 – 35.

[Til3] van Tilborg, H.C.A (1981) **The smallest length of binary 7-dimensional linear codes with prescribed minimum distance**, Discrete Math. **33,** 197 – 207.

[Tit] Tits, J. (1962) **Ovoides et groupes de Suzuki**, Arch. Math. **13**, 187-198.

[Ve] Verhoeff, Tom (1985) **Updating a table of bounds on the minimum distance of binary linear codes**, Eindhoven University of Technology Report 85-WSK-01.

[Ve2] Verhoeff, Tom (1987) **An updated table of minimum distance bounds for binary linear codes**, IEEE Trans. Inform. Theory **33,** 665 – 680.