Τμήμα Μαθηματικών
Πανεπιστήμιο Κρήτης

Το κεντρικό γραμμικό πρόβλημα της θεωρίας κωδίκων

Μάριος Μαγιολαδίτης

Ηράκλειο 2003

Διάλεξη που δόθηκε στις **4 Φεβρουαρίου 2003** στα πλαίσια του μεταπτυχιακού μαθήματος «Κωδικοποίηση» κατά τη διάρκεια του χειμερινού εξαμήνου 2002-2003. Διδάσκων: Ι. Α. Αντωνιάδης.

Το κείμενο, στο μεγαλύτερο μέρος του, αποτελεί απόδοση στα ελληνικά του κεφαλαίου 14 (σελ. 175 – 190) του βιβλίου Raymond Hill, **A First Course in Coding Theory**, Oxford University Press, 1986.

Περιεχόμενα

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)-κώδικας πάνω από το πεπερασμένο σώμα $\mathbf{F}_q$. 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)-κώδικας πάνω από το $\mathbf{F}_q$.

(Η συνάρτηση $B_q(n, d)$ παρουσιάζεται εν συντομία στις ασκήσεις 5.8. και 5.9 του βιβλίου)

Προφανώς, επειδή οι γραμμικοί κώδικες είναι διανυσματικοί υπόχωροι του $\mathbf{F}_q^{n\ 1}$ 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]-κώδικας πάνω από το GF(q).

(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]-κώδικας πάνω από το GF(q).

Η λύση της πρώτης εκδοχής για κάθε n είναι ισοδύναμη με τη λύση της δεύτερης εκδοχής για κάθε r, γιατί και στις δύο περιπτώσεις τότε 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 γίνει επακριβώς στο θεώρημα 14.3.

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

(Βλέπε και παρατήρηση 3 του κεφαλαίου 8 του βιβλίου όπου φαίνεται ότι το πρόβλημα έχει αρκετό ενδιαφέρον σε άλλους κλάδους των μαθηματικών, κυρίως στις πεπερασμένες γεωμετρίες).

[1] Στο βιβλίο του R. Hill ο διανυσματικός χώρος $\mathbf{F}_q^n$ αναφέρεται σαν V(n, q)

Ορισμοί 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.

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

Απόδειξη Έστω C ένας κώδικας τύπου [n, n – r, d] στο $\mathbf{F}_q$ με πίνακα ελέγχου ισοτιμίας H. Ο H είναι ένας r x 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 (βλέπε θεώρημα 8.4 του βιβλίου). 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 σχηματίζουμε έναν r x n πίνακα H με στήλες τα διανύσματα του K, τότε, (πάλι από το θεώρημα 8.4) ο H είναι ο πίνακας ελέγχου ισοτιμίας ενός [n, n – r]-κώδικα με ελάχιστη απόσταση το λιγότερο d.

Πόρισμα 14.2 Αν μας δοθούν τα q, d και r τότε η μεγαλύτερη τιμή για το n έτσι ώστε να υπάρχει ένας [n, n – r, d]-κώδικας στο $\mathbf{F}_q$ είναι $\max_{d-1}(r, q)$.

Οπότε το MLTC 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 14.3 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]-κώδικας ως προς το σώμα $\mathbf{F}_q$ (πόρισμα 14.2) 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]-κώδικας που θα σήμαινε ότι $n \leq \max_{d-1}(r-1, q)$, το οποίο είναι άτοπο λόγω της υπόθεσης.

Ας κάνουμε μια παύση για να σκιαγραφήσουμε τι θα κάνουμε στο υπόλοιπο κεφάλαιο.

Θα ασχοληθούμε με το MLCT πρόβλημα για αυξανόμενες τιμές της ελάχιστης απόστασης d. Οι περιπτώσεις d = 1 και d = 2 είναι εύκολες (δες και άσκηση 14.2). Θα θεωρήσουμε το πρόβλημα αρχικά 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. [Για αυτή την πολύ ενδιαφέρουσα περίπτωση βλέπε κεφάλαιο 15 του βιβλίου].

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 $B_q(n, 1) = q^n$.

- Για d = 2. Θεωρούμε το γραμμικό κώδικα $C = \{x_1x_2 \ldots x_n \mid x_1 + x_2 + \ldots + x_n = 0\}$. 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 $B_q(n, 2) = q^{n-1}$.

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

Θεώρημα 14.4 Για δοσμένο πλεόνασμα r, το μέγιστο μήκος n ενός [n, n – r, 3]-κώδικα πάνω από το $\mathbf{F}_q$ είναι $\frac{q^r-1}{q-1}$ που σημαίνει ότι $\max_2(r, q) = \frac{q^r-1}{q-1}$.

Απόδειξη Από το πόρισμα 14.2 η απαιτούμενη τιμή του n για να υπάρχει ένας γραμμικός [n, n – r, 3]-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 είδαμε στην κατασκευή των κωδίκων Hamming πάνω από το GF(q) στο κεφάλαιο 8, 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 ένα είναι πολλαπλάσιο ενός άλλου 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 14.3 και 14.4

Θεώρημα 14.5

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

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

Παρατηρήσεις

(1) Είναι εύκολο να εκφραστεί το $B_q(n, 3)$ επακριβώς συναρτήσει των q και n. Συγκεκριμένα, $B_q(n, 3) = q^{[n-\log_q(nq-n+1)]}$. (Δες και την άσκηση 14.3 στο βιβλίο του Hill).

Απόδειξη

Από το θεώρημα 14.4 υπάρχει [n, n – r, 3]-κώδικας από το $\mathbf{F}_q$ 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 για 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) την οποία θα ορίσουμε αμέσως τώρα.

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.

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

$$P = \{\lambda\mathbf{a} \mid \lambda \in GF(q)\}.$$

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

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

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

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

Λήμμα 14.6 Στο PG(r – 1, q),

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

(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 $\dfrac{q^{r-1} - 1}{q - 1}$ ευθείες.

(v) το πλήθος των (t + 1)-χώρων[2] που περιέχουν έναν δοσμένο t-χώρο είναι $\dfrac{q^{(r-1)-t} - 1}{q - 1}$.

[2] Ένας **t-χώρο** (t-space) του PG(r – 1, q) να είναι ένας υπόχωρος του $\mathbf{F}_q^r$ διάστασης t + 1 (δες ορισμό στην σελίδα 19)

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 τα λ και μ είναι 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

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

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(m, 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(m, q) το πλήθος των (t + 1)-χώρων που περιέχουν έναν δοσμένο t-χώρο είναι

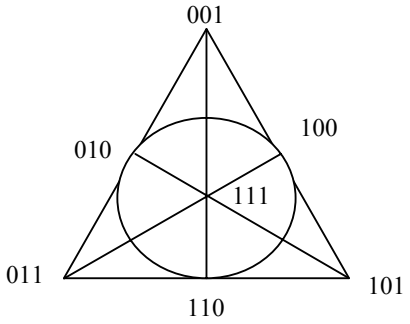
$$\frac{\frac{q^{r}-q^{t+1}}{q-1}}{\frac{q^{t+2}-q^{t+1}}{q-1}}=\frac{q^{r}-q^{t+1}}{q^{t+2}-q^{t+1}}=\frac{q^{t+1}\left(q^{(r-1)-t}-1\right)}{q^{t+1}(q-1)}=\frac{q^{(r-1)-t}-1}{q-1}.$$

Ορισμός Την προβολική γεωμετρία PG(2, q) την ονομάζουμε **προβολικό επίπεδο** πάνω από το GF(q).

Παρατήρηση Έπεται από το λήμμα 14.6 ότι η PG(2, q) είναι μια συμμετρική $(q^2 + q +1, q + 1, 1)$-κατασκευή, άρα είναι ένα προβολικό επίπεδο όπως ορίστηκε στο κεφάλαιο 2. (Βλέπε κεφάλαιο 2 σελίδα 26 του βιβλίου του Hill).

Παραδείγματα 14.7

(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 14.8



Σχήμα 14.8 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) 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 $\mathbf{F}_2^r$

Ορισμός 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

(1) Δύο βασικά πλεονεκτήματα του να δουλεύουμε στο PG(r – 1, q) είναι
(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 (δες παράδειγμα 14.7(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

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

Το MLTC πρόβλημα για d = 4

Το μέγιστο μήκος ενός [n, n – r, 4]-κώδικα ως προς το σώμα $\mathbf{F}_q$, 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)). (Εφαρμογή του πορίσματος 14.2 για d = 4).

Ένα (n, 3)-σύνολο στο επίπεδο PG(2, q) συνήθως ονομάζεται **n-τόξο** (n-arc), ενώ ένα (n, 3)-σύνολο στο επίπεδο PG(r – 1, q) για r > 3 ονομάζεται **n-cap**.

Ένα cap λέγεται **πλήρες** (complete) αν δεν περιέχεται σε ένα μεγαλύτερο cap του ίδιου προβολικού χώρου. 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 για όλα τα r, και για r ≤ 4 για όλα τα q. Αλλά, παρόλο που το πρόβλημα απέσπασε πολλή την προσοχή, λύθηκε επιπλέον μόνο για τα ζευγάρια (r, q) = (5, 3) και (6, 3). Πρόσφατα, 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 14.9 Οι γνωστές τιμές του $\max_3(r, q)$

Στη συνέχεια θα αποδείξουμε τα πιο άμεσα από αυτά τα αποτελέσματα.

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

Απόδειξη Η απόδειξη του θεωρήματος 2.7 ισχύει και για γραμμικούς κώδικες. Αυτό συμβαίνει γιατί ένας εκτεταμένος ("extended") γραμμικός κώδικας (δηλαδή ο κώδικας που παίρνεται από έναν γραμμικό κώδικα με την προσθήκη σε κάθε κωδική 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.

Για την αντίθετη κατεύθυνση, ακριβώς όπως και στο θεώρημα 2.7, διαλέγουμε στον κώδικα [n + 1, k, d + 1] κωδικές λέξεις **x** και **y** τέτοιες ώστε d(**x**, **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.

Πόρισμα 14.11 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 14.10.
(ii) Έχουμε ισοδύναμα

$n \le \max_{d-1}(r, 2)$
υπάρχει δυαδικός $[n, n - r, d]$-κώδικας
υπάρχει δυαδικός $[n - 1, n - r, d - 1]$-κώδικας
$n - 1 \le \max_{d-1}(r - 1, 2)$
$n \le \max_{d-1}(r - 1, 2) + 1$

Πόρισμα 14.12 $\max_3(r, 2) = 2^{r-1}$.

Απόδειξη

Από το θεώρημα 14.4 για q = 2 έχουμε ότι $\max_2(r, 2) = \frac{2^r - 1}{2 - 1} = 2^r - 1$. Οπότε, από το πόρισμα 14.11(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 $\hat{H}am(r - 1, 2)$ (όπως είδαμε στο κεφάλαιο 8 του βιβλίου), 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.

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 14.13 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 $[q + 2, q – 2, 4]$-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).

<u>Απόδειξη</u>

(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 και είναι γραμμικά ανεξάρτητες από τα θεωρήματα 11.1[3] και 11.2[4]. 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

[3] Θεώρημα 11.1 Ένας πίνακας Vandermonde έχει μη-μηδενική ορίζουσα
[4] Θεώρημα 11.2 Ένας r x r πίνακας με μη-μηδενική ορίζουσα έχει τις r στήλες του γραμμικά ανεξάρτητες.

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 $a_i - a_j$. Επομένως, αν $a_i \neq a_j$ 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 Α 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, $a_i^2 - a_j^2 = (a_i - a_j)^2$. (Δες και την άσκηση 3.12). Επομένως, αν $a_i \neq a_j$ η ορίζουσα det A είναι μη-μηδενική.

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

Πόρισμα 14.14 $\max_3 (3, q) \geq \begin{cases} q + 1 \text{ αν q περιττός} \\ q + 2 \text{ αν q άρτιος} \end{cases}$

Παρατήρηση Το (q +1)-τόξο που σχηματίζεται από τις στήλες του Η του θεωρήματος 14.13 είναι η κωνική τομή $\{(x, y, z) \in PG(2, q) \text{ όπου } yz = x^2\}$.

✓ Τώρα θα δείξουμε ότι οι κώδικες/τόξα που δίνονται στο θεώρημα 14.13 είναι βέλτιστοι.

Θεώρημα 14.15

(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 Η ο πίνακας ελέγχου ισοτιμίας, στην κανονική του μορφή, ενός γραμμικού [n, n – 3, 4]-κώδικα C πάνω από το $\mathbf{F}_q$ 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 = 3 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

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

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, $n - 3 \le q - 1$ οπότε $n \le q + 2$.

(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

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

όπου τα $b_1, b_2, \dots, b_{q-1}$ είναι όλα τα μη-μηδενικά στοιχεία του $\mathbf{F}_q$ και τα $c_1, c_2, \dots, c_{q-1}$ 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 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 το – 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 (Δες και την άσκηση 3.13 στο βιβλίο του Hill). Αλλά τότε

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

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

Δευτέρη 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 14.6(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 $q + 2$ διανύσματα 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 <u>ακριβώς</u> μια από αυτές. Άρα αν t από αυτές τις ευθείες τέμνουν το K σε δύο σημεία τότε $|K| = 2t$, άρτιος. Είναι <u>άτοπο</u> γιατί $|K| = q + 2$ περιττός.

Παρατήρηση 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 GF(q) και επομένως δίνει κάποια άνω φράγματα για το μέγεθος των n-τόξων για οποιοδήποτε προβολικό επίπεδο με τάξη q.

Το πόρισμα 14.14 και το θεώρημα 14.15 μας δίνουν το

Θεώρημα 14.16 (Bose 1947)

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

Παρατήρηση Ο Serge (1954) 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.

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

Θα κάνουμε μια γεωμετρική προσέγγιση του προβλήματος, για αυτό θα εισάγουμε κάποιες επιπλέον έννοιες που αφορούν στην προβολική γεωμετρία PG(r – 1, q).

Ας θυμηθούμε ότι, όταν ορίζαμε το PG(r – 1, q) από τον διανυσματικό χώρο $\mathbf{F}_q^r$, τα σημεία και οι ευθείες στο PG(r – 1, q) ήταν, αντίστοιχα, οι μονοδιάστατοι και δισδιάστατοι υπόχωροι του $\mathbf{F}_q^r$.

- 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 μια λιγότερη 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 $\frac{q^{t+1}-1}{q-1}$.

- 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 14.17 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 14.6(v) Από την ευθεία L περνάνε q + 1 επίπεδα (δες και την άσκηση 14.4 του βιβλίου) 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 14.15(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 14.18 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

$$Q = \{(0, 0, 0, 1), (x, y, 1, x^2 - by^2) \text{ όπου } x, y \in \mathbf{F}_q\} \quad (14.19)$$

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 $a_2 = (x_2, y_2, 1, x_2^2 - by_2^2)$ 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 14.17 και 14.18 μας δίνουν το

Θεώρημα 14.20 Αν q περιττός τότε $\max_3(4, q) = q^2 + 1$.

Παράδειγμα 14.21 Στο θεώρημα 14.18 θέτουμε q = 3 και b = – 1. Από την σχέση (14.19), 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 H είναι ο πίνακας ελέγχου ισοτιμίας του τριαδικού (ternary) γραμμικού [10, 6, 4]-κώδικα ο οποίος έχει μέγιστο μήκος για d = 4 και r = 4.

Παρατηρήσεις

(1) Το σύνολο Q του θεωρήματος 14.18 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.
(2) Για $q = 2^h$ με h > 1 ισχύει επίσης ότι $\max_3(4, q) = q^2 + 1$ αλλά η απόδειξη είναι λίγο πιο δύσκολη και παραλείπεται. Θα δώσουμε μόνο τα βασικά βήματα: Αρχικά δείχνεται ότι αν $q = 2^h$ (h > 1) τότε $\max_3(4, q) \le q^2 + q + 2$ ύστερα ότι δεν υπάρχει n-cap στο PG(3, q) με $q^2 + 1 < n \le q^2 + q + 2$. Τέλος, κατασκεύασε ένα $(q^2 + 1)$-cap στο PG(3, q) για q άρτιο.

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

Με την χρήση του θεωρήματος 14.3[5] μπορούμε να μεταφράσουμε άμεσα τα αποτελέσματα που βρήκαμε για το $\max_3(r, q)$ για r = 2 και 3 (πόρισμα 14.14) σε αποτελέσματα για το $B_q(n, 4)$.

Θεώρημα 14.22

Αν q περιττός τότε

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

Αν q άρτιος τότε

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

[5] Θεώρημα 14.3 Αν $\max_{d-1}(r – 1, q) < n \le \max_{d-1}(r, q)$ τότε, $B_q(n, d) = q^{n-r}$ (δες σελίδα 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 14.9 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 $\max_3(5, 4) = 41$.

- Για μια κωδικοθεωρητική απόδειξη του δεύτερου αποτελέσματος, όπου φαίνεται και η μοναδικότητα ενός βέλτιστου τριαδικού γραμμικού [56, 50, 4]-κώδικα, δες Hill (1978)

Είναι εύκολο να κατασκευάσουμε 20-caps στο PG(4, 3) (δες άσκηση 14.9 στο βιβλίο του R. Hill) 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).

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 14.21. Ένα 20-cap στο PG(4, 3) παράγεται από τις στήλες του πίνακα

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

O Hill (1983) απέδειξε ότι προβολικά υπάρχουν 9 διαφορετικά 20-caps στο PG(4, 3).

Κάνοντας χρήση του λήμματος 14.6(v) θα δείξουμε ότι το 56 είναι το μέγιστο δυνατό μέγεθος ενός cap στο PG(5, 3). (Δες και τις ασκήσεις 14.10 και 14.11 στο βιβλίο του R. Hill).

Σύμφωνα με το λήμμα 14.6(v) στο PG(5, 3) επομένως ισχύουν τα ακόλουθα

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

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

c) Ένα δοσμένο στερεό περιέχεται σε $\dfrac{3^{5-3}-1}{3-1} = \dfrac{8}{2} = 4$ 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 $|K| \leq 8 + 4(20 - 8) = 56$.

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

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

το οποίο μας δείχνει ότι το πρόβλημα εύρεσης βέλτιστων caps στο PG(6, 3) είναι πολύ μακριά από την λύση του. Η βελτίωση του φράγματος από 163 σε 136 έγινε μάλιστα φέτος, το 2003, με τη χρήση ηλεκτρονικών υπολογιστών από κοινού από τους J. Barát, Y. Edel, R. Hill και L. Storme[6]. Σε προηγούμενη εργασία τους έδειξαν ότι έδειξαν ότι κάθε 53-cap στο PG(5, 3) περιέχεται σε ένα 56-cap και ότι υπάρχουν πλήρη 48-caps στο PG(5, 3). Με αυτό τον τρόπο έριξαν το άνω φράγμα στο 154. Στην τελευταία 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 $\max_3(7, 3) \leq 147$. Η απόδειξη ολοκληρώθηκε με την χρήση υπολογιστών.

Ο G. Tallini (1964) έδειξε ότι το 41 είναι ένα κάτω φράγμα για το $\max_3(5, 4)$. Το 1999 οι Yves Edel και Jürgen Bierbrauer απέδειξαν ότι δεν υπάρχουν 42-caps στο PG(4, 4) και επομένως ότι $\max_3(5, 4) = 41$. Πιο συγκεκριμένα αρχικά έδειξαν ότι αν υπάρχει κάποιο 42-cap, έστω K, στο PG(4, 4) τότε υποχρεωτικά υπάρχει ένα υπερπεπίπεδο H το οποίο τέμνει το K το λιγότερο σε 13 σημεία Το $K \cap H$ είναι και αυτό cap στο PG(3, 4) το οποίο μάλιστα έχει το πολύ 17 σημεία. Αυτή η παρατήρηση συνέβαλε στο να αποκλειστεί, με την χρήση υπολογιστών, η ύπαρξη 42-cap στο PG(4, 4). 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

10000213010223333122103103230321021023032
01000132101013221322010121332022301101303
00100303223220123321330101023302112102012
00010032111103331223101030223133210010212
00001130331132032231021013303320332120102

[6] Στο βιβλίο του R. Hill (1986) αναφέρεται ως άνω φράγμα το 163, το οποίο ήταν και το γνωστό φράγμα μέχρι το 2000.

Ο παραπάνω πίνακας είναι ο γεννήτορας πίνακας ενός $[41, 5, 28]_4$ κώδικα. Αν, επιπλέον, συμβολίσουμε με A_i το πλήθος των κωδικών λέξεων βάρους i τότε

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

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

10000112213322333222333020022100311310012
01000100200210110110130300230321231311222
00100012002001101101103302003312213311222
00010110011100011111111111111111111101011
00001001111122222211133333300022222200113

Τα βάρη των κωδικών λέξεων κατανέμονται ως εξής:

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

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

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

Τελικά συμπεράσματα

(1) Αναφέραμε προηγουμένως ότι το πρόβλημα προσδιορισμού του max_s (r, q) πρώτη φορά απασχόλησε τον Bose (1947). Πολύ 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 Hirschfeld (1983). Για μια κατανοητή κάλυψη της θεωρίας των προβολικών γεωμετρικών πάνω από πεπερασμένά σώματα δείτε Hirschfeld (1979 και τόμος 2, υπό έκδοση).
(2) Πρόσφατα κυκλοφόρησε (1998) και μια ανανεωμένη έκδοση του βιβλίου του Hirschfeld **Projective Geometries over Finite Fields**.
(3) Για πρόσφατα αποτελέσματα που αφορούν στο max_s (r, q) για $q = 3$ και $s \leq r \leq 15$, δείτε Games (1983).
(4) Δεν φαίνεται να υπάρχει κάποιο pattern για 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 του κεφαλαίου 15.
(5) Μια άλλη εκδοχή του MLTC προβλήματος είναι η εύρεση, για δοσμένα q, n και k, η μέγιστη τιμή του d για την οποία υπάρχει ένας [n, k, d]-κώδικας στο $\mathbf{F}_q$. 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 το Verhoeff, T. (1985) **Updating a table of bounds on the minimum distance of binary linear codes**, Eindhoven University of Technology Report 85-WSK-01 ή το πιο πρόσφατο 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
(6) Το βιβλίο του R. Hill κυκλοφόρησε το 1999 με διορθώσεις.

Βιβλιογραφία

Πέρα από το βιβλίο Raymond Hill, **A First Course in Coding Theory**, Oxford University Press, 1986 υπάρχουν αναφορές στα:

Barát János, Edel Yves, Hill R. and Storme L. (submitted) **On complete caps in the projective geometries over F_3 II: New improvements**, Designs, Codes and Cryptography (Διαθέσιμο στο διαδίκτυο: http://www.mathi.uni-heidelberg.de/~yves/Papers/PG(6,3).html)

Barlotti, A. (1955) **Un estensione del theorema di Serge-Kustaanheimo**, Boll. Un. Mat. Otal. **10**, 96-98.

Bose, R. C. (1947) **Mathematical theory of the symmetrical factorial design**, Sankhya **8**, 107-166.

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)

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

Edel, Yves and Bierbrauer J. (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)

Fenton, N. E. and Vámos, P. (1982) **Matroid interpretation of maximal k-arcs in projective spaces**, Rend. Mat. (7) **2**, 573-80.

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.

Helgert, H. J. and Stinaff, R. D. (1973) **Minimum distance bounds for binary linear codes**, IEEE Trans. Info. Theory **19**, 344-356.

Hill, R. (1973) **On the largest size of cap in $S_{5,3}$**, Atti Accad. Naz. Lincei Rendiconti **54**, 378-384.

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.

Hirschfeld, J. W. P. (1979) **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.

Hirschfeld, J. W. P. (1979) **Projective geometries over finite fields**, Oxford University Press. (Διαθέσιμο από την βιβλιοθήκη του Παν. Κρήτης κωδικός: QA471.H58).

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).

Pellegrino, G. (1970) **Sul massimo ordine delle calotte in $S_{4,3}$**, Matematiche (Catania) **25**, 1-9.

Qvist, B. (1952) **Some remarks concerning curves of the second degree in a finite plane**, Ann. Acad. Sci. Fenn., Ser.A, no. 134, 1952.

Serge, B. (1954) **Sulle ovalli nei plani lineari finiti**, Atti Accad. Naz. Lincei Rendiconti **17**, 1-2

Tallini, G. (1964) **Calotte complete di $S_{4,q}$ contenenti due quadriche ellittiche quali sezioni iperpiane**, Rend.Mat e Appl. **23**, 108-123.

Verhoeff, T. (1985) **Updating a table of bounds on the minimum distance of binary linear codes**, Eindhoven University of Technology Report 85-WSK-01.