4. Ασυμπτωτικά καλές ακολουθίες καμπύλων και κωδίκων

Έστω C ένας γραμμικός κώδικας τύπου $[n, k, d]_q$.

Υπενθυμίζουμε ότι n είναι το μήκος του κώδικα, k η διάστασή του και d η ελάχιστη απόσταση του κώδικα. Το σώμα ως προς το οποίο θεωρούμε τον κώδικα είναι το $\mathbf{F}_q$.

Υπενθυμίζουμε, επίσης, ότι ο λόγος $R = \frac{k}{n}$ λέγεται **λόγος πληροφορίας** (information rate) και ο λόγος $\delta = \frac{d}{n}$ **σχετική ελάχιστη απόσταση** (relative minimal distance) του κώδικα.

Από θεώρημα της προηγούμενης παραγράφου έχουμε

$k = degG - g + 1$
$d \geq n - degG$

Προσθέτουμε κατά μέλη και έχουμε

$$k + d \geq n - g + 1$$

Διαιρούμε με n και έχουμε

$$\frac{k}{n} + \frac{d}{n} \geq 1 - \frac{g-1}{n}.$$

Δηλαδή,

$$\boxed{R + \delta \geq 1 - \frac{g-1}{n}}$$

Ορισμός 2.4.1 Έστω μια ακολουθία $(C_m , m \in \mathbf{N})$ κωδίκων τύπου $[n_m, k_m, d_m]_q$. Η ακολουθία θα λέγεται **ασυμπτωτικά καλή** όταν και μόνο όταν για $m \to \infty$ έχουμε $n_m \to \infty$ και η ακολουθία $\frac{d_m}{n_m}$ συγκλίνει σε κάποια μη-μηδενική σταθερά δ, ενώ η ακολουθία $\frac{k_m}{n_m}$ συγκλίνει σε κάποια μη-μηδενική σταθερά R.

Έστω τώρα

$$V_q := \{(\delta(C), R(C)) \in [0, 1]^2 \text{ όπου C γραμμικός κώδικας ως προς το } \mathbf{F}_q\}$$

και

$U_q \subseteq [0,1]^2$ το σύνολο των οριακών σημείων (σημείων συσσώρευσης) του V_q.

Κάνοντας χρήση αποκλειστικά στοιχειωδών τεχνικών ο Manin απέδειξε , το 1981, την ακόλουθη

Πρόταση 2.4.2 Υπάρχει μια συνεχής συνάρτηση $\alpha_q : [0, 1] \to [0, 1]$ τέτοια ώστε

Επιπλέον ισχύουν:

(i) $\alpha_q(0) = 1$.

(ii) $\alpha_q(\delta) = 0$, αν $1 - \frac{1}{q} \leq \delta \leq 1$.

(iii) Η συνάρτηση α_q είναι φθίνουσα για δ στο διάστημα $0 \leq \delta \leq 1 - \frac{1}{q}$.

Σημείωση 2.4.3 Στο ερώτημα ποια είναι η ακριβής τιμή $\alpha_q(\delta)$ για $0 \leq \delta \leq 1 - \frac{1}{q}$, δεν μπορούμε να δώσουμε σαφή απάντηση. Παρά ταύτα, μπορούμε να δώσουμε κατώτερα και ανώτερα φράγματα της τιμής αυτής.

Τα φράγματα αυτά είναι συνέπεια των αντιστοίχων ομώνυμων φραγμάτων που διατυπώσαμε στην αρχή του μαθήματος και της μελέτης της συνάρτησης εντροπίας. Η συνάρτηση αυτή χρησιμοποιείται στη θεωρία της πληροφορίας σαν ένα μέτρο μέτρησης της «αβεβαιότητας» (uncertainty).

Ορισμός 2.4.4 Η **q – αδική συνάρτηση εντροπίας** H_q: $[0, 1 - \frac{1}{q}] \to \mathbf{R}$ ορίζεται ως εξής: $H_q(0) = 0$ και

$H_q(x) := x - \log_q(q - 1) - x \log_q(x) - (1 - x)\log_q(1 - x)$, για $0 < x \leq 1 - \frac{1}{q}$.

Ισχύει η ακόλουθη:

Πρόταση 2.4.5

(α) (Φράγμα του Plotkin)

Για $0 \leq \delta \leq 1 - \frac{1}{q}$,

$$\alpha_q(\delta) \leq 1 - \frac{q}{q-1}\delta$$

(β) (Φράγμα του Hamming)

Για κάθε δ, $0 \leq \delta \leq 1$ έχουμε:

$$\alpha_q(\delta) \leq 1 - H_q(\frac{\delta}{2})$$

(γ) (Φράγμα Bassalygo – Elias)

Για $0 \le \delta \le 1 - \frac{1}{q}$ ισχύει:

$$\alpha_q(\delta) \le 1 - H_q(\theta - \sqrt{\theta(\theta - \delta)}), \text{ όπου } \theta := 1 - \frac{1}{q}.$$

(δ) (Φράγμα Gilbert – Varshamov)

Για $0 \le \delta \le 1 - \frac{1}{q}$ ισχύει:

$$\alpha_q(\delta) \ge 1 - H_q(\delta)$$

Παρατηρήσεις 2.4.6

(1) Η απόδειξη της τελευταίας πρότασης βρίσκεται στο βιβλίο των F. J. MacWilliams και N. J. A. Sloane, δες βιβλιογραφία. Για παράδειγμα η απόδειξη του φράγματος των Gilbert – Varshamov είναι στη σελίδα 557, θεώρημα 30 και γίνεται χρήση του πορίσματος 9 της σελίδας 310.
(2) Η συνάρτηση εντροπίας μελετάται στο προπτυχιακό μάθημα «Θεωρία της πληροφορίας και κωδικοποίηση», διαλέξεις κ. Τζιρίτα.

Δίνοντας τώρα διάφορες τιμές στο δ, π.χ. 0, 0,1, 0,2, κλπ, σταθεροποιώντας ένα q, π.χ. q = 2 άρα και $1 - \frac{1}{q} = 2$ μπορούμε να σχηματίσουμε το ακόλουθο διάγραμμα μεταβολής.

ΛΕΙΠΕΙ ΤΟ ΣΧΗΜΑ

Παρατηρήσεις 2.4.7

(1) Το φράγμα Gilbert – Varshamov είναι κατώτερο φράγμα κατά τα άλλα τρία ανώτερα. Από αυτά καλύτερο είναι το Bassalygo – Elias.
(2) Ακόμη καλύτερο ανώτερο φράγμα είναι το φράγμα των McEliece – Rodemich – Rumsey – Welch, δες βιβλίο MacWilliams και Sloane, σελίδα 563.
(3) Το φράγμα των Gilbert – Varshamov εγγυάται, για $0 \le \delta \le 1$, την ύπαρξη μακρών κωδίκων ως προς το $\mathbf{F}_q$ τέτοιων ώστε $\delta(C) \approx \delta$ και $R(C) \ge 1 - H_q(\delta) > 0$.

    Η απόδειξη της ύπαρξης του φράγματος είναι στοιχειώδης, αλλά όχι κατασκευαστική, δηλαδή δεν μας δίνει απλό, αλγεβρικό αλγόριθμο κατασκευής καλών μακρών κωδίκων.

(4) Υπάρχουν διάφοροι ασυμπτωτικά καλοί κώδικες που «πιάνουν» το φράγμα των Gilbert – Varshamov. Δες βιβλίο MacWilliams και Sloane, σελίδα 557.

Για να κατασκευάσουμε ασυμπτωτικά καλούς κώδικες χρειαζόμαστε καμπύλες μικρού γένους με πολλά $\mathbf{F}_q$-ρητά σημεία.

Ορισμός 2.4.8 Έστω $N_q(g)$ ο μέγιστος αριθμός των F_q-ρητών σημείων απόλυτα ανάγωγων μη-ιδιάζοντων προβολικών καμπύλων με γένος g ορισμένων στο σώμα F_q.

Ορίζουμε

$$A(q) := \limsup_{g\to\infty} \frac{N_q(g)}{g}$$

Από το θεώρημα των Hasse – Weil έχουμε: $|N_q(\boldsymbol{X}) - (q + 1)| \leq 2g\sqrt{q}$ όπου $N_q(\boldsymbol{X}) = \#\boldsymbol{X}(F_q)$. Επομένως,

$$A(q) \leq 2\sqrt{q}$$

Επίσης, σύμφωνα με το θεώρημα του Serre μπορούμε να γράψουμε

$$A(q) \leq [2\sqrt{q}\,]$$

Ισχύει το ακόλουθο

Θεώρημα 2.4.9 (Drinfeld – Vladnt)

$$A(q) \leq \sqrt{q} - 1$$

Παρατηρήσεις 2.4.10

(1) Το φράγμα αυτό είναι πολύ καλύτερο από τα προηγούμενα
(2) Απόδειξη μπορεί να δει ο ενδιαφερόμενος αναγνώστης στο βιβλίο του H. Stichtenoth, σελίδα 184.
(3) Αν το q είναι τέλειο τετράγωνο τότε το φράγμα Drinfeld – Vladnt είναι βέλτιστο αφού ισχύει η ισότητα. Δηλαδή, $A(q) = \sqrt{q} - 1$.
(4) Η απόδειξη του (3) είναι δύσκολη αλλά έχει βάθος. Χρησιμοποιεί προχωρημένα εργαλεία Θεωρίας Αριθμών και Αλγεβρικής Γεωμετρίας (Θεωρία modular καμπύλων). Ο ενδιαφερόμενος αναγνώστης μπορεί να δει (i) Tsafsman – Vladnt – T. Zink, Mathem. Nachrichten, vol.109, p.21-28, 1982 και (ii) το βιβλίο των Tsafsman – Vladnt.

Το A(q) μας δίνει επίσης ένα κατώτερο φράγμα για το $\delta + \alpha_q(\delta)$.

Συγκεκριμένα ισχύει η

Πρόταση 2.4.11 Αν υποθέσουμε ότι $A(q) > 1$ τότε για $0 \leq \delta \leq 1 - A(q)$ ισχύει

$$\alpha_q(\delta) + \delta \geq 1 - \frac{1}{A(q)}$$

Για απόδειξη δες H. Stichtenoth, σελίδα 207.

Αν τώρα q τέλειο τετράγωνο, επειδή $A(q) = \sqrt{q} - 1$, έχουμε το ακόλουθο

Θεώρημα 2.4.12 (Φράγμα TVZ) Αν τώρα q τέλειο τετράγωνο τότε για κάθε R υπάρχει ασυμπτωτικά καλή ακολουθία κωδίκων τέτοια ώστε η οριακή τιμή των λόγων πληροφορίας να είναι R και το όριο των σχετικών ελάχιστων αποστάσεων να είναι δ και επιπλέον να ισχύει

$$R + \delta \geq 1 - \frac{1}{\sqrt{q} - 1}$$

Τελικά, αποδεικνύεται ότι για q τέλειο τετράγωνο και $q \geq 49$ το φράγμα TVZ είναι καλύτερο από το φράγμα των Gilbert – Varshamov, σε κάποια περιοχή δ.

ΛΕΙΠΕΙ ΤΟ ΣΧΗΜΑ

Αυτό το αποτέλεσμα ήταν η αιτία για την έναρξη ισχυρού ενδιαφέροντος μελέτη; της θεωρίας αλγεβρογεωμετρικών κωδίκων. Τέλος, κατά τα έτη 1995-97 οι A. Garcia και H. Stichtenoth σε μια σειρά από πολύ σημαντικές εργασίες ((i) Inv. Math., vol.121, p.211-222, 1995, (ii) IEEE Trans. Information Theory, vol.41, p.1548-1563, 1995 (iii) C. R. Acad. Paris, vol. 392, p. 1067-1070, 1996, (iv) Journal of Number Theory, vol.61, p.248-273, 1996) κατασκεύσαν ακολουθίες ασυμπτωτικά καλών καμπυλών. Μειονέκτημα μέχρι σήμερα αποτελεί το γεγονός ότι το γένος των καμπυλών δεν είναι γνωστό, δίνεται μόνο ένα κατώτερο φράγμα, καθώς και ότι δύσκολα κατασκευάζονται κώδικες.