Αλγεβρικές καμπύλες και κωδικοποίηση

Γιάννης Α. Αντωνιάδης

1. Κωδικοποίηση

(1) Με q θα συμβολίζουμε κάποια δύναμη πρώτου και με $\mathbb{F}_q$ το σώμα με q στοιχεία.

(2) **Αλφάβητο** θα είναι το σύνολο των στοιχείων του σώματος $\mathbb{F}_q$ τα δε στοιχεία του θα λέγονται **γράμματα**.

(3) **κ-μήνυμα** θα λέγεται κάθε πεπερασμένη ακολουθία $a_1, a_2, ..., a_k$ στοιχείων του σώματος $\mathbb{F}_q$ μήκους k .

(4) **Κωδική λέξη** θα λέγεται κάθε ακολουθία $x = x_1, x_2, ..., x_k, x_{k+1}, ..., x_n$ στοιχείων του $\mathbb{F}_q$ μήκους n, όπου $n \geq k$ και όπου $x_1 = a_1, x_2 = a_2, ..., x_k = a_k$. Τα γράμματα $x_{k+1}, ..., x_n$ θα λέγονται **σύμβολα ελέγχου**.

(5) Αν στείλλουμε το διάνυσμα x και ο αποδέκτης λάβει y τότε το διάνυσμα $y - x$ θα λέγεται **διάνυσμα λάθους**.

(6) **Ορισμός** Ένας $[n, k]$-κώδικας C θα είναι ένα οποιοδήποτε υποσύνολο του $\mathbb{F}_q^n$, $C \subseteq \mathbb{F}_q^n$. Αν είναι και $\mathbb{F}_q$-διανυσματικός χώρος θα λέγεται **γραμμικός** $[n, k]$-κώδικας.

(7) **Απόσταση** $Hamming$:Αν $x = x_1, x_2, ..., x_n$ και $y = y_1, y_2, ..., y_n$ δύο κωδικές λέξεις, η απόσταση $Hamming$ αυτών $d_H(x, y) = card\{i \in \mathbb{N}/x_i \neq y_i\}$.

(8) **Βάρος** της κωδικής λέξης x , $W_H(x)$,ορίζεται η απόσταση $d_H(x,0)$.

(9) **Ελαχίστη απόσταση** του κώδικα C ορίζεται $d_{min}(C) = min_{x \neq y} d_H(x,y)$.

(10) Αν d είναι η ελαχίστη απόσταση γραμμικού κώδικα C τότε γράφουμε $[n,k,d]$. Αποδεικνύεται ότι ένας τέτοιος κώδικας ανιχνεύει μέχρι το πολύ $(d-1)$ -λάθη και διορθώνει μέχρι το πολύ $t = \left[\frac{d-1}{2}\right]$ λάθη.

(11) **Σφαίρα του** $Hamming$: $S_r(x) = \{y \in \mathbb{F}_q^n : d_H(x,y) \leq r\}$

(12) **Φράγμα του** $Hamming$: Ενός κώδικα C δίνονται τα q,n,t όπως παραπάνω και έστω M το πλήθος των στοιχείων του κώδικα. Ισχύει η ανισοϊσότητα $M\Bigg(1 + (q-1)\binom{n}{1} + ... + (q-1)^t\binom{n}{t}\Bigg) \leq q^n$

(13) **Φράγμα του** $Singleton$:Αν C γραμμικός κώδικας τύπου $[n,k,d]$ τότε ισχύει $k \leq n-d+1$.

Καλοί κώδικες

(1) Να ισχύει η ισότητα στο φραγμα του$Hamming$

(2) Να ισχύει η ισότητα στο φράγμα του $Singleton$. Οι κώδικες αυτοί λέγονται MDS κώδικες. (Maximum Distance Separable)

Ερώτηση

Πώς θα το επιτύχουμε;

Απάντηση

Κάνοντας χρήση αλγεβρικών καμπυλών
με πολλά ρητά σημεία.

2. Αλγεβρικές καμπύλες

(1) Αν K σώμα, $\overline{K}$ η αλγεβρική θήκη αυτού, $f(X,Y) \in K[X,Y]$ και $degf = d$, το σύνολο $C_f(\overline{K}^2) = \{(a,b) \in \overline{K}/f(a,b) = 0\}$ θα λέγεται (αφινική) **αλγεβρική καμπύλη** ορισμένη από το f βαθμού d.

(2) Φυσικά, για κάθε ενδιάμεσο σώμα $K \subseteq L \subseteq \overline{K}$ ορίζεται η $C_f(L)$.

(3) Συνήθως η μελέτη γίνεται προβολικά, ορίζουμε ομογενείς συντεταγμένες $[X,Y,Z]$ κατά τα γνωστά και το πολυώνυμο ορισμού σαν $F(X,Y,Z) \in K[X,Y,Z]$, ομογενές πολυώνυμο βαθμού d.

(4) Για $d = 1$ η καμπύλη λέγεται ευθεία, για $d = 2$ κωνική τομή, για $d = 3$ κυβική καμπύλη κ.ό.κ.

(5) Ένα σημείο $P = [x,y,z] \in C_F(\overline{K})$ της καμπύλης θα λέγεται **ιδιάζων** ακριβώς τότε όταν $F_X(P) = F_Y(P) = F_Z(P) = 0$.

(6) Η καμπύλη $C_F(\overline{K})$ θα λέγεται **μη-ιδιάζουσα** όταnν κάθε σημείο αυτής είναι μη-ιδιάζον.

(7) Η καμπύλη $C_F(\overline{K})$ θα λέγεται **ανάγωγη** όταν-ν το πολυώνυμο $F(X,Y,Z) \in K[X,Y,Z]$ είναι ανάγωγο.

(8) **Γένος** μιάς μη-ιδιάζουσας, ανάγωγης καμπύλης βαθμού n ορίζεται ο αριθμός
$g = \frac{(n-1)(n-2)}{2}$.

(9) **Το Θεώρημα** $BEZOUT$. Αν $C_F(\overline{K})$ και $C_{F'}(\overline{K})$ προβολικές αλγεβρικές καμπύλες βαθμού n, m αντίστοιχα δεν έχουν κοινή συνιστώσα, έχουν ακριβώς nm σημεία τομής. (Φυσικά λαμβάνεται υπόψη η πολλαπλότητα τομής.)

(10) **Παρατήρηση.** Αν η καμπύλη C_F είναι ορισμένη στό πεπερασμένο σώμα $\mathbb{F}_q$ και $P = (x, y, z)$ ένα σημείο αυτής τότε και ο $Frobenius$ $Fr(P)$ του σημείου P είναι επίσης σημείο της καμπύλης.

3. Διαιρέτες και ο L-χώρος τους

(1) **Ορισμός** Διαιρέτης (*divisor*) μιάς αλγεβρικής καμπύλης $C := C_F(\overline{K})$, D, θα λέγεται κάθε τυπικό άθροισμα της μορφής $D = \sum_{P \in C} n_P P$ όπου $n_P \in \mathbb{Z}$ σχεδόν όλοι μηδέν.

(2) **Φορέας** *support* ενός διαιρέτη D ορίζεται το σύνολο $Supp(D) = \{P \in C / n_P \neq 0\}$

(3) Ο Διαιρέτης D θα λέγεται $effective$ όταν όλοι οι συντελεστές του είναι **μη-αρνητικοί**.

(4) **Βαθμός** του διαιρέτη D ορίζεται ο ακέραιος $deg(D) = \sum_{P \in C} n_P$.

(5) Ο Διαιρέτης μιάς ρητής συνάρτησης $f \in \overline{K}(C)$ της καμπύλης C ορίζεται σαν ο διαιρέτης $< f >:= \sum n_P P$ όπου οι μη-μηδενικοί συντελεστές είναι στα σημεία P όπου η f έχει ρίζα βαθμού πολλαπλότητας n_P, $n_P > 0$ και πόλο τάξης $\mid n_P \mid$, όταν $n_P < 0$.

(6) Ο διαιρέτης μιας ρητής συνάρτησης λέγεται **κύριος διαιρέτης**.

(7) Ισχύει: Ο βαθμός μιάς ρητής συνάρτησης f είναι πάντοτε μηδέν. $deg(f) := deg(< f >) = 0$.

(8) Δύο διαιρέτες D και D' θα λέγονται **γραμμικά ισοδύναμοι** όταν η διαφορά τους είναι κύριος διαιρέτης.

(9) Ο L-χώρος του διαιρέτη D μιας καμπύλης C ορίζεται ως εξής: $L(D) := \{f \in \overline{K}(C)/ < f > +D \geq 0\}$

(10) Ο L-χώρος είναι $\overline{K}$-διαν. χώρος πεπερασμένης διάστασης, η οποία θα συμβολίζεται με $l(D)$.

Παρατήρηση: $f \in L(D)$ όταν $D = \sum n_P P$ σημαίνει ότι:

(1) Αν $n_P < 0$, τότε η f έχει ρίζα πολλαπλότητας τουλάχιστο $\mid n_P \mid$ και

(2) αν $n_P > 0$, τότε η f έχει πόλο τάξης το πολύ n_P.

4. Ρητοί διαιρέτες και το Θεώρημα

(1) Απο εδώ και κάτω οι καμπύλες θα είναι ορισμένες στο πεπερασμένο σώμα $\mathbb{F}_q$. Γνωρίζουμε ήδη ότι αν P σημείο της καμπύλης, τότε και $Fr(P)$ είναι επίσης σημείο της καμπύλης. Ένας διαιρέτης D της C θα λέγεται **ρητός** όταν για κάθε P που ανήκει στον D ο $Fr(P)$ έχει τον ίδιο συντελεστή με το P.

(2) Ο **L-χώρος ρητών διαιρετών** ορίζεται ανάλογα σαν $L(D) = \{f \in \mathbb{F}_q(C)^*/ < f > +D \geq 0\}$ Όλα τα παραπάνω συνεχίζουν να ισχύουν!

(3) Αν P_1,P_2,...,P_n ρητά σημεία της καμπύλης C, $D = P_1 + P_2 + ... + P_n$ και G κάποιος άλλος διαιρέτης με φορέα ξένο προς τον φορέα του D και βαθμό $2g - 2 < degG < n$, τότε ο γραμμικός κώδικας $C(D, G)$ μήκους n ως προς το σώμα $\mathbb{F}_q$ ορίζεται σαν η εικόνα της απεικόνισης $a : L(D) \longrightarrow F_q^n$ όπου $a(f) = (f(P_1), f(P_2), ..., f(P_n))$.

(4) **Θεώρημα** Ισχύουν:

$$k \geq deg(G) - g + 1$$

και

$$d \geq n - degG$$

.

(5) **Παρατήρηση** Αν $g = 0$ τότε ο κώδικας είναι ένας MDS κώδικας. Πράγματι, από το θεώρημα προκύπτει ότι $d \geq n - degG = n - k + 1$. Από το φράγμα $Singleton$ έχουμε $k \leq n - d + 1$, δηλαδή $d \leq n - k + 1$. Τελικά $d = n - k + 1$ ή $k = n - d + 1$. Γενικά για μικρό γένος παίρνουμε κώδικες που πλησιάζουν προς τους MDS.

(1) **Εικασία του** *Riemann*.
Αν C ανάγωγη, μη-ιδιάζουσα προβολική καμπύλη ορισμένη στο σώμα $\mathbb{F}_q$ και N_q το πλήθος των $\mathbb{F}_q$-ρητών σημείων αυτής, τότε ισχύει:

$$\mid N_q - (q+1) \mid \leq 2g\sqrt{q}.$$

(2) **Φράγμα του** *SERRE*.
Υποθέσεις οι ίδιες με το παραπάνω Θεώρημα.

$$\mid N_q - (q+1) \mid \leq \lfloor 2\sqrt{q} \rfloor g.$$

Παράδειγμα 1ο

Θεωρούμε την τετραδική καμπύλη του $Klein$ ($Kleinquartic$): $X^3Y + Y^3Z + Z^3X = 0$ στο σώμα $\mathbb{F}_8$.
Το γένος της καμπύλης είναι:

$$g = \frac{(n-1)(n-2)}{2} = \frac{(4-1)(4-2)}{2} = 3$$

Η καμπύλη είναι μη-ιδιάζουσα.
Το φράγμα του $Serre$ μας δίνει

$$\lfloor 2 \cdot \sqrt{8} \rfloor \cdot 3 = \lfloor 5.65 \rfloor \cdot 3 = 15$$

Συνεπώς $N \leq 15 + 9 = 24$.

Θα αποδείξουμε ότι η καμπύλη έχει ακριβώς 24

σημεία. Στο $\mathbb{F}_2$ η καμπύλη έχει τρία ακριβώς προβολικά σημεία, τα $[1,0,0]$, $[0,1,0]$ και $[0,0,1]$. Το $\mathbb{F}_8$ κατασκευάζεται σαν σώμα πηλίκων του δακτυλίου $\mathbb{F}_2[X]$ $modulo$ το ιδεώδες που παράγεται από το πολυώνυμο $f(X) = X^3 + X + 1$ δηλαδή $\mathbb{F}_8 = \mathbb{F}_2(\xi)$ όπου $\xi^3 = \xi + 1$. Αν μία συνιστώσα είναι ίση με μηδέν, τότε έχουμε ένα από τα τρία παραπάνω σημεία.

Έστω $P = [X, Y, Z]$ ρητό σημείο της καμπύλης με

$XYZ \neq 0$, γράφουμε $Z = 1$ και επειδή $\mathbb{F}_8^* =< \xi >$ τάξεως 7 γράφουμε το $Y = \xi^i, 0 \leq i \leq 6$ και το $X = \xi^{3i}\eta$ αντικαθιστούμε στην εξίσωση, απλοποιούμε με το ξ^{3i} και έχουμε $\eta^3+\eta+1 = 0$. Το πολυώνυμο όμως X^3+X+1 έχει ρίζες ξ, ξ^2, ξ^4 δηλαδή $\eta \in \{\xi, \xi^2, \xi^4\}$. Συνεπώς το πλήθος των σημείων είναι: $3 \cdot 7 + 3 = 24$

Κατασκευή του κώδικα Έστω $Q = [0,0,1]$. Ορίζουμε τους διαιρέτες.
Ο D είναι το άθροισμα των 23 υπολοίπων ρητών σημείων της καμπύλης. Ο $G = 10Q$. Προφανώς ισχύει ο περιορισμός
$2g - 2 < degG < n$, αφού $4 < 10 < 23$.
Επομένως $k = degG - g + 1 = 10 - 3 + 1 = 8$ και η ελαχίστη απόσταση αυτού $d \geq 23 - 10 = 13$.
Ο κώδικας που κατασκευάσαμε είναι του τύπου $[23, 8, d]$ με $d \geq 13$.
Εφαρμόζοντας την λεγόμενη αλυσιδωτή αντίδραση ($concatenate$) με τον $[4,3,2]$-απλό κώδικα ελέγχου ισοτιμίας κατασκευάζουμε κώδικα τύπου $[92, 24, 2d]$ με $d \geq 13$
Τέλος συμπιέζοντας τον κώδικα ($puncturate$)προκύπτει κώδικας του τύπου $[91, 24, 2d-1]$ με $d \geq 13$ ο οποίος για $n = 91$ και $d = 25$ αποτελεί

ΠΑΓΚΟΣΜΙΟ ΡΕΚΟΡ