Corbes amb molts punts sobre cossos finits

Xavier Xarles

Versió preliminar

0. Codis i corbes sobre cossos finits

Sigui $\mathbb{F}_q$ un cos finit amb $q = p^m$ elements, on p és un nombre primer i $m \geq 1$ (que s'anomena l'alfabet), i considerem el $\mathbb{F}_q$-espai vectorial $\mathbb{F}_q^n$ (els elements del qual anomenem paraules i n l'anomenem la llargada de les paraules). Considerem la distancia de Hamming a $\mathbb{F}_q^n$ donada per $d(x, y) := \#\{i \ : \ x_i \neq y_i\}$. El pes $\omega(x)$ d'una paraula x és la distancia a l'origen. Un codi lineal es un subespai lineal C de $\mathbb{F}_q^n$.

Direm que $C \subseteq \mathbb{F}_q^n$ és un (n, k, d)-codi si la seva dimensió és k i el mínim pes d'una paraula no zero a C és d. Associem a un tal codi els nombres entre 0 i 1 donats per $\delta := d/n$ (distancia relativa) i $R := k/n$ (taxa de transmissió).

Problema essencial de la teoria de codis: Construir una seqüència de codis C_i amb paràmetres δ_i i R_i tals que $\delta := \lim \delta_i$ i $R := \lim R_i$ són els dos diferents de zero (l'anomenarem una seqüència asimptòticament bona).

El 1973 Goppa va idear un mètode per a construir bons codis a partir de la geometria algebraica: considerem X una corba irreductible, llisa i projectiva sobre $\mathbb{F}_q$ i $P := \{P_1, \ldots, P_n\}$ un subconjunt de n punts diferents $\mathbb{F}_q$-racionals de X. Sigui L el subespai del cos de funcions $\mathbb{F}_q(X)$ de X format per les funcions que no tenen cap pol a P. Aleshores podem definir el morfisme evaluació

$$\alpha : L \longrightarrow \mathbb{F}_q^n$$

donat per $\alpha(f) := (f(P_1), \ldots, f(P_n))$. L'image de α és un codi. Més en general, si prenem D un $\mathbb{F}_q$-divisor de X podem definir

$$L(D) := \{f \in \mathbb{F}_q(X) \ : \ (f) + D \geq 0\} \cup \{0\}$$

i si $\mathrm{supp}(D)$ i P no intersecten podem definir el mateix morfisme evaluació obtenint el codi que anomenarem $C(D, P)$. Tenim que alguns dels invariants d'aquest codi es poden calcular a partir de C, P i D. Per exemple tenim:

Teorema 1 *Si el gènere de X és g i el grau de D compleix que $g \leq \deg(D) \leq n$, aleshores $k \geq \deg(D) + 1 - g$ amb igualtat si $\deg(D) \geq 2g - 1$, i $d \geq n - \deg(D)$.*

Exemple 2 *Si $X = \mathbb{P}^1$, $D = m\infty$ i $P := \mathbb{P}^1 \setminus \{\infty\}$, aleshores $L(D)$ és l'espai dels polinomis de grau com a molt m i $C(D,P)$ és un $(q, m+1, q-m)$-codi.*

Corol·lari 3 *Si fixem el nombre $\deg(D)/n$, aleshores la taxa de transmisió $R = k/n$ creix com n/g. A més a més, tenim que*

$$R + \delta \geq 1 + (1-g)/n.$$

Així doncs, per a construir bons codis necessitem corbes amb molts punts (respecte el gènere); o millor, per a construir bones seqüències de codis necessitem seqüències de corbes amb molts punts, i.e. corbes X_i tals que $\lim X_i(\mathbb{F}_q)/g(X_i) = \gamma > 0$; obtindrem així una seqüència de codis amb punt límit (R, δ) per sobre de la recta $R + \delta = 1 - 1/\gamma$.

1. Cotes per el nombre de punts de corbes sobre cossos finits

Comencem recordant el resultat clàssic de Hasse i Weil per el nombre de punts d'una corba de gènere g sobre $\mathbb{F}_q$.

Teorema 4 (Hasse-Weil) *Sigui X una corba (llisa i projectiva) sobre $\mathbb{F}_q$ de gènere g. Aleshores existeix un polinomi*

$$P_X(t) = \prod_{i=1}^{2g}(1 - \alpha_i t)$$

amb coeficients a $\mathbb{Z}$, on α_i són nombres complexos verificant $|\alpha_i| = \sqrt{q}$, tal que

$$\#X(\mathbb{F}_{q^r}) = q^r + 1 - \sum_{i=1}^{2g} \alpha_i^r.$$

De fet el polinomi en qüestió és el polinomi característic del Frobenius actuant (per exemple) al mòdul de Tate de la jacobiana de X.

Corol·lari 5 (Cota de Hasse-Weil) *Si X una corba (llisa i projectiva) sobre $\mathbb{F}_q$ de gènere g, aleshores*

$$|\#X(\mathbb{F}_q) - (q+1)| \leq 2g\sqrt{q},$$

i per tant

$$\#X(\mathbb{F}_q) \leq q + 1 + 2g\sqrt{q}$$

Exemple 6 *Considerem la corba plana X sobre $\mathbb{F}_{q^2}$ donada per l'equació homogènia (en el projectiu)*

$$x^{q+1} + y^{q+1} + z^{q+1} = 0,$$

(anomenada corba hermitiana). Aleshores el gènere de X és $q(q-1)/2$ i té exactament $q^3 + 1 = q^2 + 1 + 2gq$ punts. Així doncs la cota de Hasse-Weil s'assoleix.

Vist aquest últim exemple podríeu pensar que la cota de Hasse-Weil no és millorable. Observem primer que de fet només tenim un exemple quan q és un quadrat, i.e. quan $\sqrt{q}$ és enter, de manera que la cota de Hasse-Weil és un nombre enter. Podríem pensar que en general podrem arribar fins a la part entera de $q+1+2g\sqrt{q}$, i.e. $q+1+[2g\sqrt{q}]$. Però aquesta cota es pot millorar!

Teorema 7 (Serre) *Si X una corba (llisa i projectiva) sobre $\mathbb{F}_q$ de gènere g, aleshores*

$$\#X(\mathbb{F}_q) \leq (q+1) + g[2\sqrt{q}].$$

Demostració. Ordenem les arrels de $P_X(t)$ de manera que $\overline{\alpha_i} = \alpha_{i+g} = q/\alpha_i$ per a $1 \leq i \leq g$ (sempre es pot fer). Considerem els nombres reals estrictament positius

$$\beta_i := \alpha_i + \overline{\alpha_i} + [2\sqrt{q}] + 1,$$

que són enters algebraics. Aleshores

$$\beta := \prod_{i=1}^{g} \beta_i$$

és un nombre enter, ja que es fix per el grup de Galois de $\mathbb{Q}(\alpha_1, \ldots, \alpha_{2g})$ sobre $\mathbb{Q}$, i, com que els β_i són estrictament positius, $\beta \geq 1$.

Ara, la desigualtat entre la mitjana aritmètica i la geomètrica ens diu que

$$\frac{1}{g}\sum_{i=1}^{g} \beta_i \geq \sqrt[g]{\prod_{i=1}^{g} \beta_i} \geq 1$$

d'on tenim que

$$g \leq \sum_{i=1}^{g}(\alpha_i + \overline{\alpha_i} + [2\sqrt{q}] + 1) = \sum_{i=1}^{2g} \alpha_i + g[2\sqrt{q}] + g.$$

Aplicant el teorema de Hasse-Weil obtenim la cota buscada. $\square$

Una altre observació és que de fet la cota de Hasse-Weil (o la de Serre) sols és òptima per a gèneres baixos (comparats amb q). Per exemple, observem, tal com va fer Ihara, que si el nombre de punts de X a $\mathbb{F}_q$ és "alt", aleshores el nombre de punts a $\mathbb{F}_{q^2}$ és "baix". En efecte,

$$\#X(\mathbb{F}_{q^2}) = q^2 + 1 - \sum_{i=1}^{g}(\alpha_i^2 + \overline{\alpha_i}^2) = q^2 + 1 + 2qg - \sum_{i=1}^{g} t_i^2$$

on em denotat $t_i := \alpha_i + \overline{\alpha_i}$. Aplicant la desigualtat de Cauchy-Schwartz obtenim

$$\#X(\mathbb{F}_{q^2}) \leq q^2 + 1 + 2qg - \frac{1}{q}(\sum_{i=1}^{g} t_i)^2 = q^2 + 1 + 2qg - \frac{1}{g}(\#X(\mathbb{F}_q) - q - 1)^2.$$

Utilitzant que

$$\#X(\mathbb{F}_q) \leq \#X(\mathbb{F}_{q^2})$$

deduïm el següent teorema.

Teorema 8 (Ihara) *Si X una corba (llisa i projectiva) sobre $\mathbb{F}_q$ de gènere g, aleshores*

$$\#X(\mathbb{F}_q) \leq 1 + q + [(\sqrt{g^2 - 4\,qg + 4\,q^2 g + 8\,qg^2} - g)/2].$$

Aquest resultat es millor que la cota de Serre si $g > (q - \sqrt{q})/2$. Com a conseqüència tenim que si una corba X té exactament $(q+1) + g[2\sqrt{q}]$ punts racionals, aleshores $g \leq (q - \sqrt{q})/2$.

Finalment arribem a la idea de Serre de considerar els punts de X en totes les extensions $\mathbb{F}_{q^n}$ de $\mathbb{F}_q$ d'una manera optimal. La idea de Serre és utilitzar polinomis trigonomètrics.

Considerem com abans α_i les arrels del polinomi de Frobenius que escrivim de la forma $\alpha_i = \sqrt{q}e^{i\theta_i}$, per a certs $\theta_i \in \mathbb{R}$. Observem que

$$N_{q^n} := \#X(\mathbb{F}_{q^n}) = q^n + 1 - \sum_{i=1}^{g} (\alpha_i^n + \overline{\alpha_i}^n) = q^n + 1 - q^{n/2} \sum_{i=1}^{g} 2\cos(n\theta_i),$$

d'on tenim que

$$N_q \left(\frac{1}{\sqrt{q}}\right)^n \leq N_{q^n} \left(\frac{1}{\sqrt{q}}\right)^n = (\sqrt{q})^n + \left(\frac{1}{\sqrt{q}}\right)^n - \sum_{i=1}^{g} 2\cos(n\theta_i).$$

Donat $n_0 \geq 1$, considerem una successió de nombres reals $u_n \geq 0$, amb els $u_n = 0$ per a tots els $n \geq n_0$, tals que el polinomi trigonometric

$$f(\theta) := 1 + 2\sum_{n=1}^{\infty} u_n \cos(n\theta) \geq 0$$

per a tota $\theta \in \mathbb{R}$. Prenem ara $\psi(t) := \sum_{n=1}^{\infty} u_n t^n$ (és un polinomi en t).

Observació 9 $f(\theta) = \psi(e^{i\theta}) + \psi(e^{-i\theta}) + 1$

Exemple 10 *Amb $n_0 = 1$ el millor polinomi possible és $\psi(t) = \frac{1}{2}t$. Amb $n_0 = 2$ tenim ja infinites opcions, per exemple $\psi(t) = \frac{2}{3}t + \frac{1}{3}t^2$.*

Multiplicant les desigualtats anteriors per u_n i sumant respecte n tenim que

$$N_q \psi\left(\frac{1}{\sqrt{q}}\right) \leq \sum_{n=1}^{\infty} u_n N_{q^n} \left(\frac{1}{\sqrt{q}}\right)^n = \psi(\sqrt{q}) + \psi\left(\frac{1}{\sqrt{q}}\right) +$$

$$+ \sum_{i=1}^{g} \left(-2\sum_{n=1}^{\infty} u_n \cos(n\theta)\right) = \psi(\sqrt{q}) + \psi\left(\frac{1}{\sqrt{q}}\right) + \sum_{i=1}^{g} (1 - f(\theta_i)).$$

i utilitzant que $1 - f(\theta) \leq 1$ obtenim finalment la fórmula

$$N_q \psi\left(\frac{1}{\sqrt{q}}\right) \leq \psi(\sqrt{q}) + \psi\left(\frac{1}{\sqrt{q}}\right) + g.$$

Exercici 11 *Per a* $\psi(t) = \frac{1}{2}t$ *obtenim la cota de Hasse-Weil. Per a* $\psi(t) = \frac{2}{3}t + \frac{1}{3}t^2$ *obtenim la cota*

$$N_q \leq \frac{2q\sqrt{q} + q^2}{2\sqrt{q}+1} + 1 + \frac{3q}{2\sqrt{q}+1}g.$$

(per exemple, per a $q = 2$ *aquesta cota és millor que la cota de Serre per a tot* $g \geq 2$*.)*

El problema és ara trobar una successió de u_n òptims. Si fixem q i el nombre de punts N_q el problema de trobar els u_n que minimitzen g és bàsicament un problema de programació lineal que va ser resolt per Oesterlé. No posarem el resultat aquí però si es vol es pot consultar el article de Schoof ([**Sch**],Theorem 7.3). El que si que farem serà utilitzar aquest resultat per a la següent secció.

Un altre problema que no tractarem aquí es l'estudi de les corbes que assoleixen la cota de Hasse-Weil, anomenades corbes maximals; el lector pot consultar per exemple [**vdG**], secció 7, i les referències que conté.

2. Cotes asimptòtiques per el nombre de punts de corbes sobre cossos finits

Recordem que el nostre objectiu no és només trobar corbes amb molts punts si no trobar successions de corbes amb molts punts amb gènere creixent (sobre un cos fixat $\mathbb{F}_q$). Definim així

$$N_q(g) := \max\{\#X(\mathbb{F}_q) \ : \ X \text{ corba de gènere } g\ \}$$

i

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

El nostre primer objectiu és calcular aquest limit. El teorema següent ens dona la cota més bona trobada fins ara.

Teorema 12 (Drinfeld-Vladut)

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

Observem que la cota de Hasse-Weil sols ens dona $A(q) \leq 2\sqrt{q}$, així que la millora és prou gran. De fet, en el cas que q és un quadrat, tenim una igualtat, resultat que demostrarem en el cas que $q = p^2$.

Farem la demostració del teorema utilitzant la idea de Serre que hem explicat al final de la secció anterior; la demostració original de Drinfeld i Vladut és diferent (i potser més obscura); podeu consultar-la a [**Ste**],Theorem 6.23.

Demostració. Recordem que teníem

$$N_q\psi\left(\frac{1}{\sqrt{q}}\right) \leq \psi(\sqrt{q}) + \psi\left(\frac{1}{\sqrt{q}}\right) + g,$$

d'on obtenim que

$$A(q) \leq \frac{1}{\psi\left(\frac{1}{\sqrt{q}}\right)}$$

Observem que com més grans siguin els u_n que surten a la definició de $\psi(t) = \sum_{n=1}^{\infty} u_n t^n$, millor cota obtindrem. Ara bé, de la condició

$$f(\theta) := 1 + 2\sum_{n=1}^{\infty} u_n \cos(n\theta) \geq 0$$

no és difícil de veure que $u_n \leq 1$. Per tant la millor opció seria prendre tots els u_n iguals a 1; però així no tindríem un polinomi! El que fem és considerar una successió de polinomis ψ_N per a cada N de manera que els seus coeficients es vagin aproximant a 1 a mesura que $N \to \infty$. Per exemple podem prendre

$$\psi_N(t) := \sum_{i=1}^{N} \left(\frac{N+1-i}{N+1}\right) t^i.$$

Aleshores es verifica que

$$1 + \psi_N(t) + \psi_N(t^{-1}) = \frac{1}{N+1}(1 + t + \cdots + t^N)(1 + t^{-1} + \cdots + t^{-N})$$

d'on es dedueix que els $\psi_N(t)$ verifiquen la condició buscada.

Deduïm per tant que

$$A(q) \leq \lim_{N\to\infty} \frac{1}{\psi_N\left(\frac{1}{\sqrt{q}}\right)} = \frac{1}{\sum_{n=1}^{\infty}\left(\frac{1}{\sqrt{q}}\right)^n} = \sqrt{q} - 1 \qquad \square$$

3. Construcció explícita de torres de corbes amb molts punts

L'objectiu d'aquesta secció és construir explícitament torres de corbes amb molts punts basant-nos en els mètodes de A. García i H. Stichtenoth (**[Gar-Sti]**, **[Sti]**). Primer de tot farem un canvi de llenguatge: enlloc de considerar les corbes X considerarem el seu cos F de funcions racionals; els punts $\mathbb{F}_q$-racionals de X correspondran aleshores a les places racionals de F i.e. les valoracions discretes de F amb cos residual $\mathbb{F}_q$.

Així el nostre objectiu serà construir torres de cossos

$$\mathcal{F} := \{\mathbb{F}_q \subseteq F_0 \subseteq F_1 \subseteq \cdots \subseteq F_n \subseteq \cdots\}$$

de manera que cada extensió $F_n/\mathbb{F}_q$ és de grau de transcendència 1 i tal que $\mathbb{F}_q$ és algebraicament tancat a F_n, F_{n+1}/F_n és una extensió separable de grau > 1, i $\lim g(F_n) = \infty$, on $g(F_n)$

denota el gènere de F_n (de fet, només imposant que $g(F_n) > 2$ per algun n, l'ultima condició ja es verifica).

Anomenarem $N(F_n)$ el nombre de places racionals de F_n. Definim

$$\lambda(\mathcal{F}) := \lim_{n\to\infty} N(F_n)/g(F_n)$$

i direm que $\mathcal{F}$ és asimptòticament bona (òptima) si $\lambda(\mathcal{F}) > 0$ $(= \sqrt{q} - 1)$.

Lema 13 *Un torre $\mathcal{F}$ és asimptòticament bona si i només si existeixen constants $c_1, c_2 > 0$ tals que*

$$(\mathbf{A})\ g(F_n) \leq c_1[F_n : F_0] \quad i \quad (\mathbf{B})\ N(F_n) \geq c_2[F_n : F_0]$$

per a tot $n > 0$.

Demostració. La suficiencia es evident. L'altre implicació surt de la fórmula del gènere de Hurwitz: si $n \geq j \geq 0$ tenim que

$$g(F_n) - 1 = [F_n : F_j](g(F_j) - 1) + \frac{1}{2}\deg(\mathrm{Diff}(F_n/F_j)) \geq [F_n : F_j](g(F_j) - 1)$$

on $\mathrm{Diff}(F_n/F_j)$ és la diferent de F_n/F_j. Considerem també la estimació trivial $N(F_n) \leq [F_n : F_0]N(F_0)$.

Com que $\lim N(F_n)/g(F_n) > 0$, aleshores existeix un $\epsilon > 0$ tal que $N(F_n)/g(F_n) > \epsilon$ per a tot n, d'on, utilitzant les acotacions anteriors, obtenim el resultat buscat. $\square$

A més, sota les hipòtesis del Lema tindrem que $\lambda(\mathcal{F}) \geq c_1/c_2$.

La condició $(\mathbf{B})$ es fàcil de verificar: per exemple, si tenim un conjunt de places racionals S de F_0 que descomponen totalment a F_n per a tot n, aleshores $N(F_n) \geq \#S[F_n : F_0]$.

La condició $(\mathbf{A})$ és molt més delicada: cal controlar molt bé el grau $\deg(\mathrm{Diff}(F_n/F_0))$ de la diferent de F_n/F_0.

Direm que una plaça P de F_0 és no ramificada a $\mathcal{F}$ si és no ramificada a totes les extensions F_n/F_0; en cas contrari direm que és ramificada. Considerem el conjunt

$$V(\mathcal{F}) := \{P \mid P \text{ és una plaça de } F_0 \text{ ramificada a } \mathcal{F}\ \}.$$

Aleshores tenim que

$$\deg(\mathrm{Diff}(F_n/F_0)) = \sum_{P\in V(\mathcal{F})} d_n(P)$$

on

$$d_n(P) := \sum_{Q_n/P} d(Q_n/P) \cdot deg(Q_n)$$

on la suma es mou dins de totes les places Q_n de F_n a sobre de P i $d(Q_n/P)$ és l'exponent de la diferent de Q_n sobre de P. Per exemple, si l'index de ramificació $e(Q_n/P)$ de Q_n sobre P és primer amb p, aleshores $d(Q_n/P) = e(Q_n/P) - 1$; en general tenim que $d(Q_n/P) \geq e(Q_n/P) - 1$.

Utilitzant aquestes notacions i la fórmula de Hurwitz obtenim el següent criteri en el cas moderadament ramificat.

Lema 14 *Suposem que $V(\mathcal{F})$ és finit, el gènere de F_0 és 0 i que F_n/F_0 és moderadament ramificada per a tot $n \geq 0$, aleshores*

$$\lambda(\mathcal{F}) \geq \frac{2\#S}{v-2},$$

on $v := \sum_{P \in V(\mathcal{F})} \deg(P)$.

Demostració. En efecte, si F_n/F_0 és moderadament ramificada, aleshores $d_n(P) \leq [F_n : F_0]\deg(P)$, i per tant, aplicant la fórmula de Hurwitz,

$$g(F_n) - 1 = [F_n : F_0](g(F_0) - 1) + \frac{1}{2}\sum_{P \in V(\mathcal{F})} d_n(P) \leq [F_n : F_0]\left(\frac{1}{2}v - 1\right).$$

D'altre banda tenim que $N(F_n) \geq [F_n : F_0]\#S$, i així obtenim

$$\frac{N(F_n)}{g(F_n)} \geq \frac{\#S}{\frac{1}{2}v - 1 + \frac{1}{[F_n:F_0]}}$$

d'on tenim finalment que

$$\lambda(\mathcal{F}) = \lim_{n\to\infty} \frac{N(F_n)}{g(F_n)} \geq \frac{\#S}{\frac{1}{2}v - 1} \qquad \square$$

Anem a veure un mètode general per a construir torres de cossos.

Estratègia 15 *Comencem escollint un polinomi irreductible en dues variables $\varphi(X,Y) \in \mathbb{F}_q[X,Y]$ que sigui separable en X i en Y, i construïm la següent torre de cossos definida recursivament com*

$$F_0 := \mathbb{F}_q[x_0] \quad F_{n+1} := F_n[x_{n+1}]/(\varphi(x_n, x_{n+1})) \quad \text{si } n > 0.$$

La idea principal és que el cos $F := \mathbb{F}_q[X,Y]/(\varphi(X,Y))$ conté molta de la informació necessaria de la torre $\mathcal{F} := (F_n)$.

Exemple 16 *Si el grau en X i el grau en Y de $\varphi(X,Y)$ són diferents, aleshores la torre $\mathcal{F}$ no és asimptòticament bona, o sigui $\lambda(\mathcal{F}) = 0$.*

Anem a veure alguns exemples concret de torres asimptòticament bones.

Exemple 17 *Suposem que q és un quadrat, $q = r^2$, amb $r > 2$. Considerem la torre de cossos sobre $\mathbb{F}_q$ definida recursivament pel polinomi*

$$\varphi(X,Y) := Y^{r-1} + (X+1)^{r-1} - 1$$

o sigui que $F_n := \mathbb{F}_q[x_0, \ldots, x_n]$ *amb les relacions*

$$x_{i+1}^{r-1} = 1 - (1 + x_i)^{r-1} \quad \textit{per a} \quad 0 \leq i \leq n-1,$$

o sigui que l'extensió F_n/F_{n-1} *consisteix en adjuntar una arrel* $(r-1)$*-èsima* x_n *de* $1 - (1 + x_{n-1})^{r-1}$. *És clar que cada una de les extensions es moderadament ramificada (observeu que cada extensió* F_n/F_{n-1} *és una extensió de Kummer).*

Anem a calcular $V(\mathcal{F})$ *i* $S(\mathcal{F})$*. L'única plaça racional que descompon totalment a* F_n/F_0 *és* ∞*, així que* $\#S = 1$.

D'altre banda, no es difícil veure utilitzant les propietats de les extensions de Kummer que $V(\mathcal{F})$ *és igual a les places* α *a* $\mathbb{F}_q(X)$ *que ramifiquen a* $F/\mathbb{F}_q(X)$*, que a la vegada és corresponen als zeros de* $(X+1)^{r-1} - 1$ *més* ∞*; per tant* $v \leq r$*. Així, aplicant el lemma 14, tenim que*

$$\lambda(\mathcal{F}) \geq 2/(r-2),$$

que és la cota de Drinfeld-Vladut per a $q = 9$.

Exemple 18 *Com abans ens situem en el cas que el nombre d'elements del cos és un quadrat* $q = r^2$. *Considerem la torre de cossos sobre* $\mathbb{F}_q$ *definida recursivament pel polinomi*

$$\varphi(X, Y) := (Y^r + Y)(X^{r-1} + 1) - X^r$$

o sigui que $F_n := \mathbb{F}_q[x_0, \ldots, x_n]$ *amb les relacions*

$$x_{i+1}^r + x_{i+1} = \frac{x_i^r}{x_i^{r-1} + 1} \quad \textit{per a} \quad 0 \leq i \leq n-1,$$

que són recobriments d'Artin-Schreier.

Resultats clàssics de les extensions d'Artin-Schreier ens permeten provar que

$$V(\mathcal{F}) = \{\textit{Punts } \alpha \textit{ de } \mathbb{P}^1_{\mathbb{F}_q} \;\mid \alpha = \infty \textit{ o bé } \alpha^r + \alpha = 0\}$$

i

$$S(\mathcal{F}) = \{\textit{Punts } \beta \textit{ a } \mathbb{P}^1(\mathbb{F}_q) \;\mid \beta^r + \beta \neq 0\}.$$

Així tenim que

$$\#V(\mathcal{F}) = r + 1 \quad i \quad \#S(\mathcal{F}) = q - r = r^2 - r.$$

Un càlcul molt laboriós degut a la ramificació salvatge fet a ***[Gar-Sti]*** *demostra que*

$$d_n(P) \leq 2[F_n : F_0]$$

per a tot $P \in V(\mathcal{F})$. *Tenim per tant que*

$$N(\mathcal{F}) \geq \#S[F_n : F_0] = (r^2 - r)[F_n : F_0]$$

i

$$g(F_n) - 1 \leq [F_n : F_0](-1) + \frac{1}{2}(\sum_{P \in V(\mathcal{F})} d_n(P)) \leq [F_n : F_0](\#V - 1) = r[F_n : F_0]$$

d'on obtenim finalment que

$$\lim_{i \to \infty} N(F_i)/g(F_i) = \frac{r^2 - r}{r} = r - 1$$

i per tant és una torre asimptòticament òptima.

Exemple 19 *Finalment inclourem un exemple molt senzill en el cas que $q = p^2$, amb $p \neq 2$. Considerem la torre de cossos sobre $\mathbb{F}_q$ definida recursivament pel polinomi*

$$\varphi(X, Y) := 2XY^2 - X^2 - 1.$$

És clar que la torre és moderadament ramificada i verifica que

$$V(\mathcal{F}) = \{\, 0\,,\ \infty\,,\ \pm 1\,,\ \pm i\,\}$$

(on i denota una arrel quadrada de -1), i hi ha exactament $2(p-1)$ places racionals que descomponen totalment. Obtenim així del lema 14 que

$$\lambda(\mathcal{F}) \geq \frac{4(p-1)}{6-2} = p - 1$$

i per tant $\mathcal{F}$ és asimptòticament òptima.

Bibliografia

[Gar-Sti] A. García and H. Stichtenoth, *On the asymptotic behaviour of some tower of function fields over finite fields*, J. Number Theory, **61** (1996), 248–273.

[Sch] R. Schoof, *Algebraic curves and coding theory*, UTM, 336, Univ. Trento, 1990.

[Ste] S. A. Stepanov, *Codes on Algebraic Curves*, Kluwer Academic, 1999.

[Sti] H. Stichtenoth, *Algebraic Function Fields and Codes*, Universitext, Springer-Verlag, 1993.

[Sti] H. Stichtenoth, *Explicit Constructions of Towers of Function Fields with Many Rational Places*, Proceedings of the 3ecm, 2000.

[vdG] G. van der Geer, *Curves over Finite Fields and Codes*, Proceedings of the 3ecm, 2000.

Xavier Xarles
Departament de Matemàtiques
Universitat Autònoma de Barcelona
08193 Bellaterra, Barcelona, Spain
e-mail: xarles@mat.uab.es