Tours de Corps de Classe

Virgile Ducet

IML

Lundi 6 *février* 2012

Soit $C/\mathbb{F}_q$ une courbe. Soit $N(C) = |C(\mathbb{F}_q)|$.

Borne de Hasse-Weil-Serre :

$$|N(C) - q - 1| \leqslant g(C) \cdot 2\sqrt{q}.$$

Définition :
Soit $N_q(g) = \max_{g(C)=g} N(C)$. On définit la *constante d'Ihara :*

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

Remarque :
$HWS \Rightarrow A(q) \leqslant 2\sqrt{q}$.

Borne de Drinfel'd-Vlăduț (1983) :

$$A(q) \leqslant \sqrt{q} - 1.$$

Question : Comment trouver une borne inférieure pour $A(q)$?

Première approche (géométrique) : trouver des courbes de genre arbitrairement grand avec beaucoup de points.

Ihara,Tsfasman-Vlăduț-Zink (1981) : Sur $\mathbb{F}_{p^{2r}}$, il existe C de genre arbitrairement grand tel que

$$N(C) \geqslant (p^r - 1)(g(C) - 1).$$

Conséquence :

$$A(p^{2r}) = p^r - 1.$$

Zink (1985) :

$$A(p^{3r}) \geqslant \frac{2(p^{2r} - 1)}{p^r + 2} \approx 2(p^r - 1).$$

Pour q général, il faut changer de méthode :

Deuxième approche (arithmétique) : construire une suite de corps de fonctions qui à la limite aura beaucoup de places rationnelles.

Définition :
Une *tour sur* $\mathbb{F}_q$ *est une suite strictement croissante de corps de fonctions* $\mathcal{K} = (K_0, K_1, \ldots, K_n, \ldots)$ *sur* $\mathbb{F}_q$ *telle que :*

- $\forall i \geqslant 0$, K_{i+1}/K_i *est séparable ;*
- $\exists i_0 : g(K_{i_0}) > 1$.

Première méthode : Soient $F(Y) \in \mathbb{F}_q[Y]$, $G(X) \in \mathbb{F}_q(X)$. On pose $K_0 = \mathbb{F}_q(x_0)$. On définit par récurrence : si $K_i = \mathbb{F}_q(x_0, \cdots, x_i)$, alors $K_{i+1} = K_i(x_{i+1})$, où x_{i+1} vérifie

$$F(x_{i+1}) = G(x_i).$$

Exemple :
Si $q = p^{2r}$, la tour définie récursivement par :

$$F(Y) = Y^q + Y \text{ et } G(X) = \frac{X^q}{X^{q-1} + 1}$$

est *optimale (Garcia-Stichtenoth 1995) :*

$$\lim_{i \to \infty} \frac{N(K_i)}{g(K_i)} = p^r - 1 = \sqrt{q} - 1.$$

Elkies a prouvé qu'elle était aussi modulaire.

Conjecture (Elkies 1997) : toute tour récursive optimale sur $\mathbb{F}_{q^{2r}}$ est modulaire.

Deuxième méthode (plus générale, moins forte) : On va considérer des tours de corps de classe.

Corps de Classe : permet de construire des extensions abéliennes de ramification contrôlée (partie existence de la théorie) de n'importe quel corps de fonctions K.

Exemple :
Soit $\varnothing \subsetneq S \subsetneq \mathrm{Pl}(K)$, alors il existe une unique extension abélienne finie non-ramifiée K^S de K dans laquelle toutes les places de S sont totalement décomposées, et qui est maximale pour ces propriétés. On l'appelle le *S-corps de classe de Hilbert de K*. *On a :*

$$\mathrm{Gal}(K^S/K) \cong \mathrm{Cl}(\mathcal{O}_S),$$

où $\mathcal{O}_S = \{f \in K^\times : v_P(f) \geqslant 0 \ \forall P \notin S\}$.

Remarque :

Soit L/K une extension finie de c.d.f. sur $\mathbb{F}_q$. Alors :

$$N(L) \geqslant [L : K] \cdot \#\{\text{places ratio. tot. déc.}\} + \#\{\text{places ratio. tot. ram.}\}.$$

Définition :

Soit K_0 un c.d.f. et $S_0 \subset \mathrm{Pl}(K, 1)$. On définit récursivement la

S_0-tour de corps de classe de Hilbert de K_0 : soit $K_1 \overset{def}{=} K_0^{S_0}$; si S_1 est l'ensemble des places de K_1 au-dessus de S_0, alors $K_2 \overset{def}{=} K_1^{S_1}$, etc.

Proposition :

Si la S_0-tour est infinie, alors

$$A(q) \geqslant \frac{|S_0|}{g(K_0) - 1}.$$

Preuve :

$$A(q) = \limsup_{g \to \infty} \frac{N_q(g)}{g} \geqslant \lim_{i \to \infty} \frac{N(K_i)}{g(K_i)} \geqslant \lim_{i \to \infty} \frac{[K_i : K]|S_0|}{1 + [K_i : K](g(K_0) - 1)}.$$

Question : Quand est-ce que la S_0-tour est infinie ?

Remarques :

1. Supposons que la tour s'arrête au niveau n. Alors K_n/K_0 est finie et galoisienne et

$$\mathrm{Cl}(\mathcal{O}_{S_0}) \cong \mathrm{Gal}(K_1/K_0) \cong \mathrm{Gal}(K_n/K_0)^{ab}.$$

2. Soit G un groupe. Alors

$$H_1(G, \mathbb{Z}) \cong G^{ab}.$$

Suggestion : étudier la (co)homologie galoisienne de la tour. On aimerait un critère général sur des groupes de (co)homologie pour une G-action lorsque G est *fini*. *Si on peut contredire ce critère lorsque S_0 est suffisamment petit, alors on saura que la S_0-tour est infinie.*

Problème : on ne connaît pas de tel critère sur un groupe général G. Il faut supposer que G est un l-groupe pour un nombre premier l.

Conséquence : il faut modifier la définition de la tour.

Définition :

La *(l, S_0)-tour de corps de classe de Hilbert de K_0 est définie par récurrence en prenant pour K_{i+1} la l-partie $K_i^{S_i}(l)$ de $K_i^{S_i}$, c'est-à-dire sa l-sous-extension maximale ($\mathrm{Gal}(K_{i+1}/K_i)$ est un l-groupe).*

Remarque :

Il est facile de montrer par récurrence que la (l, S_0)-tour est une sous-tour de la S_0-tour, donc l'infinitude de la première implique l'infinitude de la seconde.

Définition :

Soit G un groupe (fini). Un *G-module* M *est un* $\mathbb{Z}[G]$*-module.*

Tate associe à chaque G-module M un groupe de cohomologie $H^j(G, M)$ $(-\infty < j < \infty)$ *tel qu'à toute suite exacte courte*

$$0 \to M' \to M \to M'' \to 0$$

est associée une suite exacte (très) longue :

$$\cdots \to H^j(G, M') \to H^j(G, M) \to H^j(G, M'') \to H^{j+1}(G, M') \to \cdots$$

Exemple :

$H^{-2}(G, \mathbb{Z}) = G^{ab}$ *et* $H^{-2}(G, \mathbb{F}_l) = G^{ab}(l)$.

Définition :

On note $d_l(G) = \dim_{\mathbb{F}_l} H^{-2}(G, \mathbb{F}_l)$ *et* $r_l(G) = \dim_{\mathbb{F}_l} H^{-3}(G, \mathbb{F}_l)$.

Théorème (Golod-Šafarevič 1964) :

Si G est un l-groupe fini, alors :

$$r_l(G) > \frac{1}{4} d_l(G)^2.$$

Théorème (Serre 1985) :

Si la (l, S_0)-tour s'arrête en L_{S_0} et $G_{S_0} = \mathrm{Gal}(L_{S_0}/K_0)$, alors

$$r_l(G_{S_0}) - d_l(G_{S_0}) \leqslant |S_0| - 1 + \delta_l(q),$$

où $\delta_l(q) = 1$ si $l|(q-1)$, 0 sinon.

Corollaire :

Si la (l, S_0)-tour s'arrête, alors

$$d_l(G_{S_0}) < 2 + 2\sqrt{|S_0| + \delta_l(q)}.$$

Remarque :

On a pour tout groupe G :

$$d_l(G) = \dim_{\mathbb{F}_l} G^{ab}(l),$$

donc

$$d_l(G_{S_0}) = d_l(G_{S_0}^{ab}) = d_l(\mathrm{Gal}(K_0^{S_0}(l)/K_0)) = d_l(\mathrm{Cl}(\mathcal{O}_{S_0})).$$

Corollaire (autre formulation) :

Si

$$d_l(\mathrm{Cl}(\mathcal{O}_{S_0})) \geqslant 2 + 2\sqrt{|S_0| + \delta_l(q)},$$

alors la (l, S_0)-tour est infinie.

Question : Comment trouver des c.d.f. et des ensembles S_0 avec beaucoup de l-torsion dans le S_0-groupe de classe ?

Théorème (Schoof 1992) :

Soit L/K cyclique de degré premier l (sur $\mathbb{F}_q$), et $\rho = \#\{P : P \text{ est ramifiée}\}$. Soit $S \subset \mathrm{Pl}(K)$ et soit $T \subset \mathrm{Pl}(L)$ l'ensemble des places de L au-dessus de S. Alors

$$d_l(\mathrm{Cl}(\mathcal{O}_T)) \geqslant \rho - 1 - (|S| - 1 + \delta_l(q)) = \rho - \delta_l(q) - |S|.$$

Récapitulatif :

L/K cyclique de degré l, ρ places ramifiées, $S \subset \mathrm{Pl}(K)$, $T \subset \mathrm{Pl}(L)$ au-dessus de S. Si

$$\rho - \delta_l(q) - |S| \geqslant 2 + 2\sqrt{|T| + \delta_l(q)},$$

c'est-à-dire

$$\rho \geqslant 2 + \delta_l(q) + |S| + 2\sqrt{|T| + \delta_l(q)},$$

alors la (l, T)-tour de L est infinie, et on a

$$A(q) \geqslant \frac{|T|}{g(L) - 1}.$$

Exemple :

$K = \mathbb{F}_3(x)$ et $l = 2$: soit L/K définie par

$$y^2 = x(x+1)(x+2)(x^2+1)(x^2+x+2)(x^3+2x+1)(x^3+2x+2)(x^3+x^2+2)$$

Alors $g(L) = 7$, $\delta_l(q) = 1$, $S = \{1/x\}$, donc $|S| = 1$ et $|T| = 2$. On a bien

$$8 = \rho \geqslant 2 + \delta_l(q) + |S| + 2\sqrt{|T| + \delta_l(q)} = 2 + 1 + 1 + 2\sqrt{2+1},$$

donc la tour est infinie et

$$\sqrt{3} - 1 \geqslant A(3) \geqslant \frac{|T|}{g(L) - 1} = \frac{2}{7-1} = \frac{1}{3}.$$