BORNE DE WEIL ET GRAPHES DE CAYLEY SUR DES CORPS FINIS

Isaac KONAN, Master 1 MFA

June 13, 2015

INTRODUCTION

Considérons un corps fini $\mathbb{F}_q$, et un polynôme unitaire f dans $\mathbb{F}_q[X]$. On rappelle qu'un caractère de Dirichlet χ modulo f est le prolongement sur $\mathbb{F}_q[X]$ d'un morphisme de $(\mathbb{F}_q[X]/f\mathbb{F}_q[X])^*$ dans $\mathbb{C}^*$, en une forme multiplicative complète définie par

$$\chi(g) = \begin{cases} 0 & \text{si} \quad g \wedge f \neq 1 \\ \chi(g(mod\ f)) & \text{sinon} \end{cases}$$

pour tout g dans $\mathbb{F}_q[X]$. Le caractère de Dirichlet dit trivial est celui ne prenant que la valeur 1 sur les $g \wedge f = 1$ de $\mathbb{F}_q[X]$.
On définit également la fonction de Von Mangoldt Λ sur $\mathbb{F}_q[X]$ par

$$\Lambda(g) = \begin{cases} 0 & \text{si g n'est pas une puissance d'un irréductible de } \mathbb{F}_q[X] \\ \deg(\pi) & \text{si g est une puissance du polynôme irréductible } \pi \end{cases}$$

pour tout g dans $\mathbb{F}_q[X]$.

Théorème 0.1 (borne de Weil)**.** *Soit χ un caractère non trivial sur $\mathbb{F}_q[X]$ et $d \in \mathbb{N}^*$. On a pour les g pris unitaires*

$$|\sum_{\deg(g)=d} \Lambda(g)\chi(g)| \leq (\deg(f)-1)q^{\frac{d}{2}} \ .$$

Cette majoration est de l'ordre de $O(q^{\frac{d}{2}})$, tandis qu'une majoration grossière donnerait

$$|\sum_{\deg(g)=d} \Lambda(g)\chi(g)| \leq \sum_{\deg(g)=d} \Lambda(g) = q^d \ .$$

Cette dernière égalité est obtenue en évaluant le cardinal de

$$\{(x, \pi_x)/x \in \mathbb{F}_{q^d},\ \pi_x \text{ polynôme minimal de x}\},$$

qui vaut d'une part $\sharp\mathbb{F}_{q^d} = q^d$ par unicité du polynôme minimal, et d'autre part

$$\sum_{\pi_x}\sum_{x} 1 = \sum_{\deg(\pi)|d} \deg(\pi) = \sum_{g=\pi^{\frac{d}{\deg(\pi)}}} \Lambda(g) = \sum_{\deg(g)=d} \Lambda(g)$$

en utilisant le critère de séparabilité dans des extensions de $\mathbb{F}_q$. Notons également que

$$|\sum_{\deg(g)=d} \Lambda(g)\chi(g)| = \sum_{\deg(g)=d} \Lambda(g)$$

pour χ trivial, qui est de l'ordre de $O(q^d)$. Cette différence d'ordre suivant le fait que χ soit trivial ou non est l'élément clé de cette borne de Weil.

Le but de ce travail est d'aborder la démonstration de ce théorème sous certains critères mettant en avant une méthode astucieuse utilisée par Stepanov, et par la suite utiliser le théorème pour étudier quelques propriétés de graphes de Cayley dans des groupes $\mathbb{F}_{q^n}^*$.

1 UNE APPROCHE DE DÉMONSTRATION

1.1 Notion de fonction L

On définit la fonction L comme étant la fonction géneratrice sur l'ensemble des polynômes unitaires g de $\mathbb{F}_q[X]$ exprimée par

$$L(\chi, T) = \sum_{g \text{ un.}} \chi(g) T^{\deg(g)} \ .$$

Il s'agit ici d'une série avec

$$L(\chi, T) = \sum_{n \geq 0} \Big(\sum_{\substack{g \text{ un.} \\ \deg(g) = n}} \chi(g) \Big) T^n \ .$$

Il est clair que le coefficient constant vaut 1, le seul polynôme unitaire de degré nul étant 1.

Proposition 1.1. *Pour χ non trivial, $L(\chi, T)$ est un polynôme de degré au plus* $\deg(f) - 1$.

Preuve. Pour tout $n \geq \deg(f)$, on considère l'application définie par

$$\begin{array}{rccc} \phi_n : & \{\deg(g) = n\} & \to & \{\deg(g) = n - \deg(f)\} \times \{\deg(g) \leq \deg(f) - 1\} \\ & g & \mapsto & (q, r) \text{ avec } g = hf + r \end{array}$$

est une bijection en utilisant l'unicité de h et r par la division euclidienne mais également les propriétés du degré.
Mieux encore, comme f est unitaire, on a donc g est unitaire si et seulement si h l'est. Ainsi

$$\sharp\{\deg(g) = n,\ g = r (mod\ f),\ g \text{ un.}\} = \sharp\{\deg(g) = n - \deg(f),\ g \text{ un.}\} = q^{n - \deg(f)}$$

le choix du coefficient dominant étant fixé. On en déduit que

$$\sum_{g \text{ un}, \deg(g) = n} \chi(g) = q^{n - \deg(f)} \sum_{r (mod\ f)} \chi(r) = 0$$

par orthogonalité. □

Ce théorème montre clairement que $L(\chi, T)$ est de la forme $1 + \sum_{i=1}^{k} c_i T^i$ avec $k = \deg(f)$, et donc l'existence de complexes $\omega_1, \cdots, \omega_k$ tels que

$$L(\chi, T) = \prod_{i=1}^{k} (1 - \omega_i T) \ .$$

Ceci nous permet de trouver une première forme exponentielle à la fonction $L(\chi, T)$. On a

$$\begin{aligned} T\frac{L'(\chi,T)}{L(\chi,T)} &= \sum_{i=1}^{k} \frac{-\omega_i T}{1-\omega_i T} \\ &= -\sum_{i=1}^{k}\sum_{n\geq 1} \omega_i^n T^n \\ &= -\sum_{n\geq 1}(\sum_{i=1}^{k} \omega_i^n) T^n \ . \end{aligned}$$

En posant donc $S_n(\chi) = -\sum_{i=1}^{k} \omega_i^n$, et du fait du coefficient constant à 1, on a

$$L(\chi, T) = \exp(\sum_{n\geq 1} \frac{S_n(\chi)}{n} T^n) \ . \tag{1}$$

Proposition 1.2. *On a pour tout $n \geq 1$,*

$$S_n(\chi) = \sum_{\substack{g \text{ un.} \\ \deg(g) = d}} \Lambda(g)\chi(g) \ .$$

Preuve. L'anneau $\mathbb{F}_q[X]$ étant factoriel, on peut réécrire $L(\chi, T)$ en produit eulérien, avec

$$L(\chi, T) = \prod_{\pi \text{ ir.un.}} \frac{1}{1-\chi(\pi)T^{\deg(\pi)}} \ .$$

On a donc

$$\begin{aligned} T\frac{L'(\chi,T)}{L(\chi,T)} &= \sum_{\pi \text{ ir.un.}} \frac{\deg(\pi)\chi(\pi)T^{\deg(\pi)}}{(1-\chi(\pi)T^{\deg(\pi)})^2} \cdot (1-\chi(\pi)T^{\deg(\pi)}) \\ &= \sum_{\pi \text{ ir.un.}} \frac{\deg(\pi)\chi(\pi)T^{\deg(\pi)}}{1-\chi(\pi)T^{\deg(\pi)}} \\ &= \sum_{\pi \text{ ir.un.}} \deg(\pi) \sum_{n\geq 1} \chi(\pi)^n T^{n\cdot\deg(\pi)} \\ &= \sum_{\pi \text{ ir.un.}} \sum_{n\geq 1} \Lambda(\pi^n)\chi(\pi^n) T^{\deg(\pi^n)} \\ &= \sum_{g \text{ un.}} \Lambda(g)\chi(g) T^{\deg(g)} \\ &= \sum_{n\geq 1}(\sum_{\deg(g)=n} \Lambda(g)\chi(g)) T^n \ . \end{aligned}$$

□

Nous avons ainsi réussi à ressortir la somme à majorer de la borne de Weil. On déduit donc que pour tout $n \geq 1$,

$$|\sum_{\deg(g)=n} \Lambda(g)\chi(g)| = |\sum_{i=1}^{k} \omega_i^n| \leq k \cdot \max_{1\leq i\leq k} |\omega_i|^n \leq (\deg(f)-1)R^n$$

où $R > 0$ est tel que $\omega_1, \cdots, \omega_k \in \mathcal{B}(0,R)$. Il est donc logique de penser que R pourrait valoir $\sqrt{q}$, hypothèse faisant l'objet du théorème suivant:

Théorème 1.1 (hypothèse de Riemann pour les corps finis, A. Weil)**.** *Soit f unitaire dans $\mathbb{F}_q[X]$ et χ un caractère de Dirichlet non trivial modulo f. On a*

$$L(\chi, T) = \prod_{i=1}^{k}(1-\omega_i T)$$

sous sa forme factorisée, avec $k \leq \deg(f)-1$ et

$$|\omega_i| \leq \sqrt{q}$$

pour tout $i \in [\![1;k]\!]$.

La preuve de ce théorème entraîne immédiatement la preuve de la Borne de Weil. Bien que non évidente, on peut se restreindre à certains polynômes f et des caractères particuliers modulo f pour lesquels la démonstration du théorème sera "moins" laborieuse.

1.2 Cas particulier de caractère de Dirichlet

On considère η un caractère multiplicatif sur $\mathbb{F}_q$. Soit f un polynôme unitaire de $\mathbb{F}_q[X]$. On crée ainsi un caractère de Dirichlet dit associé à f et η vérifiant des conditions assez particulières relatives aux normes.

Proposition 1.3. *Soient η un caractère multiplicatif sur $\mathbb{F}_q$ et f un polynôme unitaire de $\mathbb{F}_q[X]$. Il existe un unique caractère de Dirichlet χ modulo f, tel que pour tout $n \in \mathbb{N}^*$ et tout x dans $\mathbb{F}_{q^n}$, on ait*

$$\eta(N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(f(x))) = \eta(-1)^{n\cdot\deg(f)}\chi(\pi_x)^{\frac{n}{\deg(\pi_x)}} ,$$

où π_x est le polynôme minimal de x.

Preuve. On procède tout d'abord à la vérification de l'unicité d'un tel caractère

unicité: $\mathbb{F}_q[X]$ étant factoriel, et un caractère de Dirichlet multiplicatif, il suffit donc de vérifier l'unicité pour les irréductibles unitaires de $\mathbb{F}_q[X]$. Soit π un tel polynôme. On pose α l'une de ses racines et l'on prend $n = \deg(\pi)$. On a donc

$$\chi(\pi) = \eta(-1)^{n\cdot\deg(f)}\eta(N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(f(\alpha))) .$$

Cette expression ne dépend aucunement de la racine choisie car toute autre racine de π est de la forme α^{q^m} car obtenue par composition du morphisme de Frobenius $x \mapsto x^q$. Ainsi,

$$N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(f(\alpha^q)) = N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(f(\alpha)^q) = N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(f(\alpha))^q = N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(f(\alpha)) \ ,$$

les normes $N_{\mathbb{F}_{q^n}/\mathbb{F}_q}$ à valeurs dans $\mathbb{F}_q$, et le morphisme de Frobenius conservant $\mathbb{F}_q$.

existence: Pour commencer, écrivons f sous sa forme factorisée. On a

$$f = \prod_{i=1}^{k} \pi_i^{l_i} \ ,$$

et on pose α_i une racine de π_i et $d_i = \deg(\pi_i)$ pour tout $i \in [\![1; k]\!]$. On définit donc le caractère χ de la manière suivante:

$$\chi(g) = \prod_{i=1}^{k} \eta(N_{\mathbb{F}_{q^{d_i}}/\mathbb{F}_q}(g(\alpha_i)))^{l_i} \ .$$

On rappelle que pour tout irréductible π ayant pour racine α, toutes les racines sont exactement les α^{q^i}, avec $i \in [\![1; \deg(\pi)]\!]$, avec $\alpha = \alpha^{q^i}$ seulement pour $i = \deg(\pi)$. On a également dans $\mathbb{F}_{q^n}/\mathbb{F}_q$, la norme $N_{\mathbb{F}_{q^n}/\mathbb{F}_q}$ qui vaut exactement pour tout x

$$N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(x) = \prod_{i=1}^{n} x^{q^i} \ .$$

On peut donc réécrire

$$\chi(g) = \prod_{i=1}^{k} \eta(\prod_{j=1}^{d_i} g(\alpha_i^{q^j}))^{l_i} = \eta(\prod_{i=1}^{k}(\prod_{j=1}^{d_i} g(\alpha_i^{q^j}))^{l_i}) \ .$$

Vérifions que χ est bien le caractère recherché. Pour tout $n \geq 1$ et tout $x \in \mathbb{F}_{q^n}$, on pose π_x son polynôme minimal. On a donc

$$\begin{aligned}
\eta(N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(f(x))) &= \eta(\prod_{t=1}^{n} f(x^{q^t})) \\
&= \eta(\prod_{t=1}^{n}\prod_{i=1}^{k}(\pi_i(x^{q^t}))^{l_i}) \\
&= \eta(\prod_{t=1}^{n}\prod_{i=1}^{k}(\prod_{j=1}^{d_i}(x^{q^t} - \alpha_i^{q^j}))^{l_i}) \\
&= \eta(\prod_{i=1}^{k}(\prod_{j=1}^{d_i}\prod_{t=1}^{n}(x^{q^t} - \alpha_i^{q^j}))^{l_i}) \ .
\end{aligned}$$

On obtient donc

$$\begin{aligned}\eta(N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(f(x))) &= \eta(\prod_{i=1}^{k}(\prod_{j=1}^{d_i}(-1)^n\prod_{t=1}^{n}(\alpha_i^{q^j}-x^{q^t}))^{l_i}) \\ &= \eta((-1)^{n\cdot\deg(f)}\prod_{i=1}^{k}(\prod_{j=1}^{d_i}\prod_{t=1}^{n}(\alpha_i^{q^j}-x^{q^t}))^{l_i}) \ ,\end{aligned}$$

car $\deg(f)=\sum_{i=1}^{k} d_i l_i$. Pour conclure, on rappelle que $\deg(\pi_x)$ divise n pour tout $x\in\mathbb{F}_{q^n}$. Ainsi, chaque racine de π_x apparaît exactement $\dfrac{n}{\deg(\pi_x)}$ dans $\{x^{q^t}/\ t\in[\![1;n]\!]\}$. On a donc pour tout y

$$\prod_{t=1}^{n}(y-x^{q^t})=(\pi_x(y))^{\frac{n}{\deg(\pi_x)}} \ .$$

Ceci nous permet de déduire que

$$\begin{aligned}\eta(N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(f(x))) &= \eta((-1))^{n\cdot\deg(f)}\cdot\eta(\prod_{i=1}^{k}(\prod_{j=1}^{d_i}\prod_{t=1}^{n}(\alpha_i^{q^j}-x^{q^t}))^{l_i}) \\ &= \eta((-1))^{n\cdot\deg(f)}\cdot\eta(\prod_{i=1}^{k}(\prod_{j=1}^{d_i}(\pi_x(\alpha_i^{q^j}))^{\frac{n}{\deg(\pi_x)}})^{l_i}) \\ &= \eta((-1))^{n\cdot\deg(f)}\cdot\eta(\prod_{i=1}^{k}(\prod_{j=1}^{d_i}\pi_x(\alpha_i^{q^j}))^{l_i})^{\frac{n}{\deg(\pi_x)}} \\ \eta(N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(f(x))) &= \eta(-1)^{n\cdot\deg(f)}\cdot\chi(\pi_x)^{\frac{n}{\deg(\pi_x)}} \ .\end{aligned}$$

□

Le caractère ainsi créé est d'autant plus intéressant par la proposition suivante:

Proposition 1.4. *Soit χ le caractère de Dirichlet associé à un polynôme unitaire f de $\mathbb{F}_q[X]$ et η un caractère multiplicatif de $\mathbb{F}_q$. On a alors pour tout $n\geq 1$*

$$\sum_{x\in\mathbb{F}_{q^n}/\mathbb{F}_q}\eta(N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(f(x)))=\eta(-1)^{n\cdot\deg(f)}\cdot S_n(\chi) \ .$$

Preuve. On a

$$\begin{aligned}\sum_{x\in\mathbb{F}_{q^n}/\mathbb{F}_q}\eta(N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(f(x))) &= \eta(-1)^{n\cdot\deg(f)}\sum_{x\in\mathbb{F}_{q^n}/\mathbb{F}_q}\chi(\pi_x)^{\frac{n}{\deg(\pi_x)}}\\ &= \eta(-1)^{n\cdot\deg(f)}\sum_{\substack{\pi \text{ ir.un.}\\ \deg(\pi)|n}}\deg(\pi)\chi(\pi)^{\frac{n}{\deg(\pi)}}\\ &= \eta(-1)^{n\cdot\deg(f)}\sum_{\substack{\pi \text{ ir.un.}\\ \deg(\pi)|n}}\Lambda(\pi^{\frac{n}{\deg(\pi)}})\chi(\pi^{\frac{n}{\deg(\pi)}})\ .\end{aligned}$$

On obtient donc la relation

$$\sum_{x\in\mathbb{F}_{q^n}/\mathbb{F}_q}\eta(N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(f(x))) = \eta(-1)^{n\cdot\deg(f)}\cdot S_n(\chi) \tag{2}$$

vu que

$$\sum_{\substack{g \text{ un.}\\ \deg(g)=n}}\Lambda(g)\chi(g) = \sum_{\substack{\pi \text{ ir.un.}\\ \deg(\pi)|n}}\Lambda(\pi^{\frac{n}{\deg(\pi)}})\chi(\pi^{\frac{n}{\deg(\pi)}})\ .$$

□

Le caractère associé χ a d'autres particularités. En effet, c'est aussi **un caractère de Dirichlet modulo f^δ le plus grand diviseur sans facteur carré de** f, la fonction multiplicative $g \mapsto g(\alpha_i)$ se faisant modulo π_i, avec

$$f = \prod_{i=1}^{k}\pi_i^{l_i}\ .$$

D'autre part, **si f n'est pas une puissance d-ième, avec $d = ord(\eta) > 1$, η non trivial, alors χ est également non trivial**. Pour s'en convaincre, on choisit i_0 tel que l_{i_0} ne soit pas un multiple de d. Comme η n 'est pas trivial et d'ordre d, on peut trouver β dans $\mathbb{F}_q$ tel que $\eta(\beta)^{l_{i_0}} \neq 1$. La fonction norme étant surjective, on peut donc trouver θ dans $\mathbb{F}_{q^{d_i}}/\mathbb{F}_q$ tel que $N_{\mathbb{F}_{q^{d_i}}/\mathbb{F}_q}(\theta) = \beta$. Un tel θ peut toujours être mis sous la forme $g_{i_0}(\alpha_{i_0})$. Enfin, en prenant par le théorème chinois

$$\begin{cases} g &= 1 \ mod(\pi_i) \text{ pour } i \neq i_0\\ g &= g_{i_0} \ mod(\pi_{i_0})\end{cases}$$

on obtient automatiquement $\chi(g) = \eta(\beta)^{l_{i_0}} \neq 1$. On a donc

Proposition 1.5. *Soient η un caractère non trivial de $\mathbb{F}_q$ d'ordre d, et f un polynôme unitaire dans $\mathbb{F}_q[X]$ qui n'est pas une puissance d-ième. Alors le caractère χ associé a pour fonction de Dirichlet $L(\chi,T) = L(f,\eta,T)$ un polynôme de degré au plus $\deg(f^\delta)-1$, où f^δ est le plus grand diviseur sans facteur carré de f.*

1.3 Méthode de Stepanov

La méthode de Stepanov consiste en une suite d'astuces visant à amoindrir la difficulté du problème. En effet, on ramène le problème au comptage d'un ensemble de points. Pour cet ensemble de points, si l'on trouve un polynôme A, tel que tout point de notre ensemble est racine de A de multiplicité un entier m fixé, alors on pourra majorer son cardinal par $\deg(A)/M$. Le choix du polynôme se fait astucieusement pour obtenir l'inégalité souhaitée.

1.3.1 Astuce 1: ne plus se limiter à un seul caractère

Lemme 1.1. *Soient $a_1, \cdots, a_m$ des complexes non nuls avec $m \geq 1$. On suppose qu'il existe $A, B > 0$, tels que pour tout $n \in \mathbb{N}^*$*

$$|\sum_{i=1}^{k} a_i^n| \leq A.M^n \ .$$

Alors $a_1, \cdots, a_m \in \overline{\mathcal{B}}(0, M)$.

Preuve. Considérons la série entière

$$F(z) = \sum_{n\geq 0}(\sum_{i=1}^{k} a_i^n)z^n \ .$$

Par hypothèse elle est définie et holomorphe sur $\mathcal{B}(0, \frac{1}{M})$. Mais on peut réecrire

$$F(z) = \sum_{n\geq 0}(\sum_{i=1}^{k} a_i^n)z^n = \sum_{i=1}^{k}\sum_{n\geq 0} a_i^n z^n = \sum_{i=1}^{k} \frac{1}{1-a_i z} \ .$$

Cette écriture n'est valable que sur des boules de rayons $R \leq \min_{1\leq i\leq k} \frac{1}{|a_i|}$ et y est holomorphe. On en déduit que $\frac{1}{M} \leq \min_{1\leq i\leq k} \frac{1}{|a_i|}$. □

Cette première astuce nous permet de directement d'évaluer des sommes $\sum_\chi S_n(\chi)$ et de conclure pour chacun des ω de chacun de ses caractères χ. L'astuce qui suit évalue une somme sur un ensemble bien précis de caractères χ.

1.3.2 Astuce 2: réduction à un comptage de points

Soient $1 < d|(q-1)$, et f un polynôme unitaire de $\mathbb{F}_q[X]$ tel $d \wedge \deg(f) = 1$. On considère l'ensemble caractère multiplicatif η non triviaux de $\mathbb{F}_q$, tels que η^d soit trivial. Il est important de remarquer que la condition $d \wedge \deg(f) = 1$ est cruciale, car c'est l'unique condition pour laquelle aucun diviseur de d différent de 1 ne divise $\deg(f)$, ce qui assure que f ne peut être une puissance d'ordre de ce dernier. Le caractère χ associé à chaque η est donc non trivial, et on a pour tout $n \geq 1$

$$-\sum_i (\eta(-1)^{\deg(f)} \cdot \omega_{i,\chi})^n = \eta(-1)^{n\cdot\deg(f)} \cdot S_n(\chi) = \sum_{x\in\mathbb{F}_{q^n}} \eta(N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(f(x)))$$

et donc

$$\sum_{\eta\neq 1,\eta^d=1}\sum_{x\in\mathbb{F}_{q^n}}\eta(N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(f(x)))=\sum_{\omega}\omega^n$$

où les ω sont égaux au module près aux $\omega_{i,\chi}$, et donc une somme finie.

Lemme 1.2 (Réduction au comptage de points)**.** *Soient $d|(q-1)$, et f un polynôme unitaire de $\mathbb{F}_q[X]$. On a pour tout $n\geq 1$*

$$\sum_{\eta\neq 1,\eta^d=1}\sum_{x\in\mathbb{F}_{q^n}}\eta(N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(f(x)))=\sharp\{(x,y)\in\mathbb{F}_{q^n}\times\mathbb{F}_{q^n}/\ y^d=f(x)\}-q^n\ .$$

Preuve. Notons tout d'abord que l'application

$$\eta\mapsto\eta\circ N_{\mathbb{F}_{q^n}/\mathbb{F}_q}$$

est un morphisme de groupe de l'ensemble des caractères de $\mathbb{F}_q$ d'ordre divisant d vers l'ensemble des caractères de $\mathbb{F}_{q^n}$ d'ordre divisant d, $(q-1|q^n-1)$. Ces deux groupes sont cycliques d'ordre d. Mieux encore, il s'agit d'un isomorphisme, puisque ce morphisme est injectif. En effet, la norme étant surjective sur $\mathbb{F}_q$, tout η non trivial donne un caractère non trivial. On peut donc réécrire

$$\sum_{\eta\neq 1,\eta^d=1}\sum_{x\in\mathbb{F}_{q^n}}\eta(N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(f(x)))=\sum_{\zeta\neq 1,\zeta^d=1}\sum_{x\in\mathbb{F}_{q^n}}\zeta(f(x))$$

avec ζ caractère dans $\mathbb{F}_{q^n}$. On a donc

$$\sum_{\eta\neq 1,\eta^d=1}\sum_{x\in\mathbb{F}_{q^n}}\eta(N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(f(x)))=\sum_{x\in\mathbb{F}_{q^n}}\sum_{\zeta\neq 1,\zeta^d=1}\zeta((f(x)))\ .$$

On rappelle que

$$\sum_{\zeta^d=1}\zeta(t)=\begin{cases}d & \text{si } t \text{ est une puissance } d\text{-ième dans } \mathbb{F}_{q^n}^*\\ 0 & \text{sinon.}\end{cases}$$

Comme $d|q^n-1$, c'est aussi le nombre de solutions de l'équation $t=u^d$ dans $\mathbb{F}_{q^n}$, pour $t\in\mathbb{F}_{q^n}^*$. Ainsi pour tout $t\in\mathbb{F}_{q^n}^*$,

$$\sum_{\zeta\neq 1,\zeta^d=1}\zeta(t)=\sharp\{u\in\mathbb{F}_{q^n}/\ u^n=t\}-1\ .$$

Pour $t=0$, on a également

$$\sum_{\zeta\neq 1,\zeta^d=1}\zeta(t)=0=\sharp\{u\in\mathbb{F}_{q^n}/\ u^n=t\}-1\ ,$$

vu que l'équation admet comme unique solution $u=0$. Pour tout t dans $\mathbb{F}_{q^n}$, on a donc

$$\sum_{\zeta\neq 1,\zeta^d=1}\zeta(t)=\sharp\{u\in\mathbb{F}_{q^n}/\ u^n=t\}-1\ .$$

On déduit ainsi le lemme énoncé

$$\sum_{\eta\neq 1,\eta^d=1}\sum_{x\in\mathbb{F}_{q^n}}\eta(N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(f(x)))=\sharp\{(x,y)\in\mathbb{F}_{q^n}\times\mathbb{F}_{q^n}/\ y^d=f(x)\}-q^n\ .$$

□

1.3.3 Astuce 3: théorème de Stepanov, Bombieri

Le théorème de Stepanov, Bombieri est l'astuce clé permettant de contourner la variable entière n. En effet pour tout $n\geq 1$, un polynôme de $\mathbb{F}_q[X]$ est également un polynôme de $\mathbb{F}_{q^n}[X]$ et le cardinal de $\mathbb{F}_{q^n}$ est q^n. Il est donc souhaitable d'évaluer $|\sharp\{(x,y)\in\mathbb{F}_q\times\mathbb{F}_q/\ y^d=f(x)\}-q|$ pour un corps donné $\mathbb{F}_q$.

Théorème 1.2 (Stepanov, Bombieri)**.** *Soit $\mathbb{F}_q$ un corps fini, extension paire de son corps premier. Soit f un polynôme non constant de $\mathbb{F}_q[X]$ et un entier $d|q-1$ tel que $d\wedge\deg(f)=1$. Alors il existe une constante $C\geq 0$ ne dépendant que de d et de $\deg(f)$, tel que*

$$|\sharp\{(x,y)\in\mathbb{F}_q\times\mathbb{F}_q/\ y^d=f(x)\}-q|\leq C\sqrt{q}\ .$$

Notons que ce théorème implique que

$$|\sum_{\omega}\omega^{2n}|\leq q^n$$

pour tout n, et donc par le **lemme 1.1** que $|\omega|^2\leq q$ pour tout ω. par passage à la racine carré on obtient le résultat souhaité.

Une astuce complémentaire est se restreindre uniquement à l'étude de $\sharp\{(x,y)\in\mathbb{F}_q\times\mathbb{F}_q/\ y^d=f(x)\}$:

Lemme 1.3 (de la borne sup à la borne inf)**.** *Soit $\mathbb{F}_q$ un corps fini. Soit f un polynôme non constant de $\mathbb{F}_q[X]$ et un entier $d|q-1$ tel que $d\wedge\deg(f)=1$. On définie $a(f)$ par*

$$\sharp\{(x,y)\in\mathbb{F}_q\times\mathbb{F}_q/\ y^d=f(x)\}=q+a(f)\ .$$

Alors

$$\sharp\{(x,y)\in\mathbb{F}_q\times\mathbb{F}_q/\ y^d=f(x)\}\geq q-(d-1)\max_{\epsilon\in\mathbb{F}_q^*}|a(\epsilon f)|\ .$$

Si l'on réussit à majorer $a(f)$ par un $C'\sqrt{q}$, avec $C'\geq 0$ ne dépendant que de d et $\deg(f)$, les ϵf étant de même degré que f, on aura

$$(1-d)C'\sqrt{q}\leq\sharp\{(x,y)\in\mathbb{F}_q\times\mathbb{F}_q/\ y^d=f(x)\}-q\leq C'\sqrt{q}$$

et donc

$$|\sharp\{(x,y)\in\mathbb{F}_q\times\mathbb{F}_q/\ y^d=f(x)\}-q|\leq C\sqrt{q}$$

pour $C=dC'$ qui ne dépendra que de d et $\deg(f)$.

Preuve. On considère le sous groupe $(\mathbb{F}_q{}^*)^d$ des puissances d-ième dans $\mathbb{F}_q{}^*$. $\mathbb{F}_q{}^*$ étant cyclique, il en est de même pour le quotient $\mathbb{F}_q{}^*/(\mathbb{F}_q{}^*)^d$, ayant exactement d éléments. Notons $\{1 = \epsilon_1, \cdots, \epsilon_d\}$ des réprésentants des classes $\mathbb{F}_q{}^*/(\mathbb{F}_q{}^*)^d$. Pour tout ϵ_i, on a

$$\sharp\{(x,y) \in \mathbb{F}_q \times \mathbb{F}_q^*/\ y^d = \epsilon_i f(x)\} = q + a(\epsilon_i f) - r(f)$$

avec $r(f)$ le nombre de racines de f dans $\mathbb{F}_q$, qui est le même que le nombre de racines de ϵf pour tout ϵ dans $\mathbb{F}_q{}^*$. D'autre part, pour tout x n'étant pas racine de f, $f(x)$ est dans $(\mathbb{F}_q{}^*)^d$ à un ϵ_i près. On a donc

$$d(q - r(f)) = \sum_{i=1}^{d} \sharp\{(x,y) \in \mathbb{F}_q \times \mathbb{F}_q^*/\ y^d = \epsilon_i f(x)\} = \sum_{i=1}^{d} q + a(\epsilon_i f) - r(f)$$

et donc

$$\sum_{i=1}^{d} a(\epsilon_i f) = 0\ .$$

Pour tout ϵ dans $\mathbb{F}_q{}^*$, $a(\epsilon f) = a(\epsilon_i f)$, pour ϵ_i le représentant de la classe de ϵ, on a donc

$$a(f) = -\sum_{i=2}^{d} a(\epsilon_i f) \geq -(d-1) \max_{\epsilon \in \mathbb{F}_q^*} |a(\epsilon f)|$$

□

L'idée émise par Stepanov était de créer un polynôme A dans $\mathbb{F}_q[X]$ qui s'annulerait pour tous les x de $\mathbb{F}_q$ admettant des solutions à $f(x) = y^d$, et de multiplicité au moins m, pour un m fixé. On aurait donc

$$\sharp\{(x,y) \in \mathbb{F}_q \times \mathbb{F}_q/\ y^d = f(x)\} \leq d \cdot \frac{\deg(A)}{m}$$

vu que $f(x) = y^d$ admet au plus d solutions à chaque x. Le problème est que les critères de multiplicité relatifs aux dérivées ne peuvent être utilisés, car $m! = 0$ dès que $m \geq p$ caractéristique de $\mathbb{F}_q$. La méthode utilisée par Stepanov fait appel aux dérivées de Hasse, pour parer à ce problème.

Bombieri propose une autre méthode, toujours dans la même logique que Stepanov, mais en passant par $\mathbb{F}_q[X,Y]$, et qui généralise le théorème de Stepanov, ce qui nous donne le nom final de Stepanov, Bombieri. C'est cette méthode que nous verrons par la suite.

1.3.4 Astuce 4: comportements dans $\mathbb{F}_q[X,Y]$

On se place dans la clôture de $\mathbb{F}_q$ notée $\overline{\mathbb{F}}_q$. On considère la courbe

$$\mathcal{C} = \{(x,y) \in \overline{\mathbb{F}}_q \times \overline{\mathbb{F}}_q/\ y^d = f(x)\}\ .$$

En posant Fr le morphisme de Frobenius $(x, y) \mapsto (x^q, y^q)$, on a donc

$$\mathcal{C}(\mathbb{F}_q) = \{(x, y) \in \mathcal{C}/\mathrm{Fr}(x, y) = (x, y)\} = \{(x, y) \in \mathbb{F}_q^2/\ y^d = f(x)\}\ .$$

Le polynôme que l'on recherche doit tout particulièrement s'annuler sur $\mathcal{C}(\mathbb{F}_q) \subset \mathcal{C}$. On se place donc dans $\mathcal{O}(\mathcal{C}) = \mathbb{F}_q[X, Y]/(Y^d - f(X))$. C'est un anneau intègre. En regardant $\mathbb{F}_q[X, Y]$ sous la forme $\mathbb{F}_q[X][Y]$, on a $Y^d - f(X)$ unitaire dans cet anneau, et on obtient par division euclidienne pour tout g dans $\mathbb{F}_q[X, Y]$ un unique reste de la forme

$$\sum_{i=0}^{d-1} = g_i Y^i,\ \text{avec}\ g_i \in \mathbb{F}_q[X]\ \ .$$

Dans $\mathcal{O}(\mathcal{C})$, tout polynôme est donc de la forme

$$\sum_{i=0}^{d-1} = g_i Y^i$$

avec $g_i \in \mathbb{F}_q[X]$. On définit donc pour un g $\mathcal{O}(\mathcal{C})$ son degré par

$$\deg(g) = \max_{g_i \neq 0}\{d \cdot \deg(g_i) + i \cdot \deg(f)\}$$

si $g \neq 0$ et $-\infty$ si $g = 0$. Cette définition tient toujours si l'on pose $\deg(0) = -\infty$ dans $\mathbb{F}_q[X]$ l'on retire la condition $g_i \neq 0$. Il peut tre difficile de cerner le fait que $\mathcal{O}(\mathcal{C})$ soit intègre, mais nous le verrons par la suite à travers les propriétés particulières de deg sur $\mathcal{O}(\mathcal{C})$. On commence tout d'abord par énoncer un lemme capital pour la suite.

Lemme 1.4. *Pour tout entier k, il existe un unique $i \in [\![0; d-1]\!]$, et un unique entier t tel que*

$$k = dt + i \cdot \deg(f)\ .$$

De plus, $t \geq 0$ dès que $k \geq (d-1)(k-1)$.

Preuve. Notons que $d \wedge \deg(f) = 1$ entraîne que $\deg(f)$ génère $\mathbb{Z}/d\mathbb{Z}$. On en déduit que pour tout k entier, il existe un unique $i\ mod(d)$ tel que

$$k = i \cdot \deg(f)\ (mod(d))$$

et donc l'existence d'un unique entier t et d'un unique $i \in [\![0; d-1]\!]$ tels que

$$k = dt + i \cdot \deg(f)\ .$$

Supposons maintenant que $t < 0$. On a donc

$$k = dt + i \cdot \deg(f) \leq -d + (d-1)\deg(f) < 1 - d + (d-1)\deg(f)$$

et donc $k < (d-1)(\deg(f) - 1)$. □

Une conséquence directe de ce lemme est que

$$\{d \cdot \deg(g_i) + i \cdot \deg(f) / \ g_i \neq 0\}$$

contient des éléments deux à deux distincts, et donc que le degré défini pour $g \in \mathcal{O}(\mathcal{C})^*$ est atteint en un unique i, d'où la proposition suivante:

Proposition 1.6. *Pour tous g_1 et g_2 dans $\mathcal{O}(\mathcal{C})$, on a*

$$\deg(g_1 + g_2) \leq \max\{\deg(g_1); \deg(g_1)\}$$

avec égalité dès que $\deg(g_1) \neq deg(g_2)$*, et*

$$\deg(g_1 g_2) = \deg(g_1) + \deg(g_2) \ .$$

La preuve est triviale en axant la démontration sur les valeurs maximales i_1 et i_2 de g_1 et g_2. On y trouve une justification à l'intégrité de $\mathcal{O}(\mathcal{C})$. On définit également une notion de multiplicité de racine de g de la façon suivante:
g de multiplicité $\geq m$ en (x, y) dans $\mathcal{C}$ avec $y \neq 0$, si

$$\frac{g}{(X-x)^m} = \frac{p}{q} \ ,$$

où p et q sont dans $\mathcal{O}(\mathcal{C})$ tels que $q(x, y) \neq 0$.

Lemme 1.5. *(x, y) un zéro de g, avec $y \neq 0$, est de multiplicité au moins* 1.

Preuve. Écrivons

$$g = \sum_{i=0}^{d-1} g_i(X) Y^i \ .$$

On a pour tout i,

$$g_i(X) = g_i(x) + (X-x)u_i(X) \text{ et } Y^i = y^i + (Y-y)v_i(Y) \ .$$

On en déduit que

$$\frac{g}{X-x} = \sum_{i=0}^{d-1} u_i(X) Y^i + \frac{\sum_{i=0}^{d-1} g_i(x) y^i}{X-x} + \frac{Y-y}{X-x} \sum_{i=0}^{d-1} g_i(x) v_i(Y) \ .$$

Comme $g(x, y) = 0$, on a donc

$$\frac{g}{X-x} = \sum_{i=0}^{d-1} u_i(X) Y^i + \frac{Y-y}{X-x} \sum_{i=0}^{d-1} g_i(x) v_i(Y) \ .$$

Or $Y^d - y^d = g(X) - g(x)$, ce qui implique que

$$\frac{Y-y}{X-x} = \frac{h(X)}{\sum_{i=0}^{d-1} Y^i y^{d-1-i}}$$

qui est défini en (x, y) dès que en $y \neq 0$. □

On définit également $r_0(g)$ de nombre de ces racines comptées avec multiplicité.

Proposition 1.7. *On a pour tout g dans $\mathcal{O}(\mathcal{C})^*$*

$$r_0(g) \leq \deg(g) \ .$$

Preuve. Notons que $d|q-1$, et donc l'ensemble des racines d-ième de l'unité est dans $\mathbb{F}_q$. Pour tout g dans $\mathcal{O}(\mathcal{C})^*$, on considère le polynôme dèfini par

$$N(g) = \prod_{\epsilon^d=1} g(X, \epsilon Y) \ ,$$

qui ne dépend pas de Y, vu que $N(g) = N(\epsilon g)$ pour tout ϵ. Il est donc à la fois dans $\mathbb{F}_q[X]$ et $\mathcal{O}(\mathcal{C})^*$. Comme $\deg(g(X, \epsilon Y)) = \deg(g)$ dans $\mathcal{O}(\mathcal{C})^*$, on a donc

$$d \cdot \deg(g) = \deg(N(g)) = d \cdot \deg_{\mathbb{F}_q[X]}(N(g))$$

et donc $\deg(g) = \deg_{\mathbb{F}_q[X]}(N(g))$.
Aussi, si (x, y) est un zéro de g, alors x est un zéro de $N(g)(X)$. En remarquant de plus que

$$\frac{g_1}{(X-x)^{m_1}} \cdot \frac{g_2}{(X-x)^{m_2}} = \frac{g_1 g_2}{(X-x)^{m_1+m_2}} \ ,$$

on a donc que la multiplicité x comme racine dans $\mathbb{F}_q[X]$est supérieure à la somme des multiplicités des $(x, \epsilon y)$ de g dans $\mathcal{O}(\mathcal{C})^*$. On déduit donc le résultat souhaité. □

Ceci est important car si toutes les racines de g dans $\mathcal{O}(\mathcal{C})^*$ sont de multiplicités au moins m, alors on a

$$\sharp\{g(x, y) = 0\} \leq \frac{\deg(g)}{m} + \deg(f)$$

en dissociant les $(x, 0)$ racines de g qui ajoute au plus au cardinal le nombre de x annulant f et donc $\deg(f)$. Si l'on réussit donc à majorer $\deg(g)/m$ par une expression de la forme $q + C\sqrt{q}$, avec C en fonction de d et $\deg(f)$, alors il en sera de même pour $\deg(g)/m + \deg(f)$ qu'on pourra majorer par $q + C'\sqrt{q}$, avec $C' = C + \deg(f)$ ne dépendant également que de d et $\deg(f)$. Nous allons donc chercher un tel polynôme g et un bon entier m, pour lesquels cette majoration est possible.

1.3.5 Astuce 5: recherche d'un polynôme dans $\mathcal{O}(\mathcal{C})^*$

On considère les entiers qui, par le **lemme 1.4**, ont une unique décomposition pour $0 \leq i \leq d-1$

$$k = dt + i \cdot \deg(f)$$

avec $t \geq 0$. Ce sont des entiers naturels, car $d, t, i, \deg(f) \geq 0$. On les ordonne en une unique suite strictement croissante

$$(k_j)_{j \in \mathbb{N}^*} \ .$$

Il est clair que tous les degrés dans $\mathcal{O}(\mathcal{C})^*$ possibles sont éléments de cette suite. De plus, pour tout $j \geq 1$, on peut écrire $k_j = dt_j + i_j \cdot \deg(f)$ de façon unique. On a donc pour $X^{t_j}Y^{i_j} = s_j$ dans $\mathcal{O}(\mathcal{C})^*$ que

$$\deg(s_j) = dt_j + i_j \deg(f) = k_j \ .$$

La suite (k_j) constitue ainsi l'ensemble des degrés possibles dans $\mathcal{O}(\mathcal{C})^*$. On remarque que $d_1 = 0$. Rappelons également que le **lemme 1.4** veut que pour tout

$$k \geq (d-1)(\deg(f)-1)$$

une telle décomposition soit possible. On en déduit donc l'existence d'une plus petite valeur, noté j_0, pour laquelle on ait $k_{j+1} = k_j + 1$ pour tout $j \geq j_0$. On a évidemment $k_{j_0} \leq (d-1)(\deg(f)-1)$.

Pour tout $k \geq 0$, on considère l'ensemble

$$\mathcal{H}(k) = \{g \in \mathcal{O}(\mathcal{C})^* / \ \deg(g) \leq k\} \cup \{0\}$$

qui, par la **proposition 1.6** est un $\mathbb{F}_q$-espace vectoriel. Il est clair que $\mathcal{H}(0) = \mathbb{F}_q$, et de donc de dimension 1. Pour un

$$g = \sum_{i=0}^{d-1} g_i(X)Y^i = \sum_{i=0}^{d-1} \sum_{j=0}^{\deg(g_i)} a_{j,i}X^jY^i$$

dans $\mathcal{H}(k)$, on a clairement dans $\mathcal{O}(\mathcal{C})^*$

$$deg(X^jY^i) \leq k$$

pour tout $0 \leq i \leq d-1$, et $0 \leq j \leq \deg(g_i)$. On a donc que $\mathcal{H}(k)$ est engendré par les s_j, pour les $k_j \leq k$. Mieux encore, il s'agit d'une base, puisque tous les k_j sont distincts. On a donc clairement que

$$\dim_{\mathbb{F}_q}(\mathcal{H}(k)) = \sharp\{k_j \leq k\} = \max_j\{k_j \leq k\} \ .$$

On en déduit directement la proposition suivante :

Proposition 1.8. *Il existe $\delta \geq 0$ un entier tel que, pour tout $k \geq k_{j_0}$, on a*

$$\dim_{\mathbb{F}_q}(\mathcal{H}(k)) = k + 1 - \delta \ .$$

En particulier

$$\delta = k_{j_o} - j_0 + 1 \leq (d-1)(\deg(f)-1) \ .$$

Pour un $\kappa \geq 0$, on considère les s_j pour $k_j \leq \kappa$. Pour chacun d'eux, l'élément

$$S_j = s_j \circ \mathrm{Fr} = \mathrm{Fr} \circ s_j = s_j^q$$

qui est également dans $\mathcal{O}(\mathcal{C})^*$ et de degré qk_j.

Proposition 1.9. *Soient $\kappa, k \geq 0$ deux entiers, et m un diviseur de q. Alors l'ensemble des fonctions*

$$h = \sum_{k_j \leq \kappa} (h_j)^m S_j \ ,$$

où les h_j sont dans $\mathcal{H}(k)$ est un sous-espace vectoriel de $\mathcal{H}(mk + q\kappa)$, noté $\mathcal{H}'(m, k, \kappa)$, qui est exactement le sous-espace vectoriel formé par les éléments de la forme $(g_1)^m(g_2 \circ \mathrm{Fr})$, où g_1 dans $\mathcal{H}(k)$ et g_2 dans $\mathcal{H}(\kappa)$.

Preuve. Il est clair que tout élément h de cette forme est dans $\mathcal{H}(mk + q\kappa)$. Supposons maintenant que

$$h = (g_1)^m(g_2 \circ \mathrm{Fr})$$

où g_1 dans $\mathcal{H}(k)$ et g_2 dans $\mathcal{H}(\kappa)$. On peut donc écrire

$$g_2 = \sum_{k_j \leq \kappa} a_j s_j \ .$$

On a donc

$$h = (g_1)^m(\sum_{k_j \leq \kappa} a_j S_j) \ ,$$

$\mathbb{F}_q$ étant fixe par Fr. De plus, $a_j = a_j^q = (a_j^{\frac{q}{m}})^m$. Comme q/m est une puissance de p, caractéristique de $\mathbb{F}_q$, $a_j^{\frac{q}{m}}$ est dans $\mathbb{F}_q$, et on en déduit que

$$h = \sum_{k_j \leq \kappa} (h_j)^m S_j \ ,$$

avec $h_j = a_j^{\frac{q}{m}} g_1$. D'autre part, si u, v dans $\mathcal{H}'(m, k, \kappa)$ et a, b dans $\mathbb{F}_q$, on a

$$a \cdot u + b \cdot v = \sum_{k_j \leq \kappa} (a(u_j)^m + b(v_j)^m) S_j = \sum_{k_j \leq \kappa} (a^{\frac{q}{m}} u_j + b^{\frac{q}{m}} v_j)^m S_j$$

qui est encore un élément de $\mathcal{H}'(m, k, \kappa)$. □

Les fonctions de cette forme sont particulières par le lemme suivant :

Lemme 1.6. *Si*

$$h = \sum_{k_j \leq \kappa} (h_j)^m S_j$$

tel que

$$\sum_{k_j \leq \kappa} (h_j)^m s_j = 0$$

dans $\mathcal{O}(\mathcal{C})$, alors $h(\mathcal{C}(\mathbb{F}_q)) = 0$, et toutes les racines sont de multiplicité au moins m.

Preuve. Il est évident que $h(\mathcal{C}(\mathbb{F}_q)) = 0$. D'autre part,

$$h = \sum_{k_j \leq \kappa} (h_j \cdot (s_j)^{\frac{q}{m}})^m = (\sum_{k_j \leq \kappa} h_j \cdot (s_j)^{\frac{q}{m}})^m$$

une puissance m-ième dans $\mathcal{O}(\mathcal{C})$. □

Nous avons ainsi résolu le problème des éléments de $\mathcal{C}(\mathbb{F}_q)$ comme racines de multiplicité au moins m d'un polynôme. La dernière idée est de s'assurer que l'écriture de h de cette forme peut être unique sous certaines conditions.

Lemme 1.7. *Soit*

$$h = \sum_j (h_j)^m S_j$$

dans $\mathcal{H}'(m, k, \kappa)$. *Si* $km < q$, *alors* $h = 0$ *si et seulement si* $h_j = 0$ *pour tout* $k_j \leq \kappa$. *En d'autres termes, cette écriture est unique dans* $\mathcal{H}'(m, k, \kappa)$.

Preuve. Par l'absurde si $h = 0$ et au moins un $h_j \neq 0$. On considère le j maximal pour lequel $h_j \neq 0$. On a

$$(h_j)^m S_j = -\sum_{j'<j} (h_{j'})^m S_{j'} \ .$$

On a d'une part

$$\deg((h_j)^m S_j) \geq \deg(S_j) = qk_j$$

et d'autre part

$$\deg(-\sum_{j'<j} (h_{j'})^m S_{j'}) \leq mk + q(k_j - 1) \ .$$

On a donc

$$qk_j \leq mk + q(k_j - 1) \ \Rightarrow \ q \leq mk$$

d'où la contradiction. □

Ainsi, pour la condition $mk < q$, on a

$$\dim_{\mathbb{F}_q}(\mathcal{H}'(m, k, \kappa)) = \dim_{\mathbb{F}_q}(\mathcal{H}(k)) \times \dim_{\mathbb{F}_q}(\mathcal{H}(\kappa)) \ .$$

Comme $\mathbb{F}_p$ est stable par tous les $x \mapsto x^{p^\alpha}$, on a donc que $\mathcal{H}'(m, k, \kappa)$ est un $\mathbb{F}_p$-espace vectoriel avec linéarité pour cette écriture. On définit donc l'application $\mathbb{F}_p$-linéaire

$$\Delta : \begin{cases} \mathcal{H}'(m, k, \kappa) & \to & \mathcal{H}(mk + \kappa) \\ \sum_{k_j \leq \kappa} (h_j)^m S_j & \mapsto & \sum_{k_j \leq \kappa} (h_j)^m s_j \end{cases}$$

Par le théorème du rang, on a

$$\dim_{\mathbb{F}_p}(\mathcal{H}'(m, k, \kappa)) = \dim_{\mathbb{F}_p}(Ker(\Delta)) + \dim_{\mathbb{F}_p}(Im(\Delta))$$

et donc

$$\dim_{\mathbb{F}_p}(\mathcal{H}'(m,k,\kappa)) \leq \dim_{\mathbb{F}_p}(Ker(\Delta)) + \dim_{\mathbb{F}_p}(\mathcal{H}(mk+\kappa)) \ .$$

On en déduit que

$$\dim_{\mathbb{F}_p}(Ker(\Delta)) \geq \dim_{\mathbb{F}_p}(\mathcal{H}'(m,k,\kappa)) - \dim_{\mathbb{F}_p}(\mathcal{H}(mk+\kappa)) \ .$$

On obtiet donc une minoration concrète de $\dim_{\mathbb{F}_p}(Ker(\Delta))$

$$\dim_{\mathbb{F}_p}(Ker(\Delta)) \geq [\mathbb{F}_q : \mathbb{F}_p][\dim_{\mathbb{F}_q}(\mathcal{H}(k)) \cdot \dim_{\mathbb{F}_q}(\mathcal{H}(\kappa)) - \dim_{\mathbb{F}_q}(\mathcal{H}(mk+\kappa))] \ .$$

1.3.6 Astuce 6: choix des paramètres

On est donc sûr qu'un élément h dans $\mathcal{H}'(m,k,\kappa)$ non nul admet pour racines de multiplicité au moins m tous les éléments convenables de $\mathcal{C}(\mathbb{F}_q)$ dès que

$$\dim_{\mathbb{F}_q}(\mathcal{H}(k)) \cdot \dim_{\mathbb{F}_q}(\mathcal{H}(\kappa)) - \dim_{\mathbb{F}_q}(\mathcal{H}(mk+\kappa)) > 0 \ . \tag{3}$$

On aurait donc pour ce h que

$$\frac{\deg(h)}{m} \leq \frac{mk+q\kappa}{m} = k + q \cdot \frac{\kappa}{m} \ .$$

Cette dernière égalité nous montre qu'il serait judicieux que κ et m soient du même ordre. Aussi dès que $m, k \geq k_{j_0}$, et $\kappa \geq m$, on a par la **proposition 1.8** une expression exacte des dimensions. Pour satisfaire à l'inégalité du théorème de Stepanov, vu que q est une puissance paire de p, on peut donc poser

$$\left\{ \begin{array}{lcl} m & = & \sqrt{q} \\ \kappa & = & \sqrt{q} + 2\delta \end{array} \right.$$

On aurait donc $mk < q \Leftrightarrow k < \sqrt{q}$, et pour (3) que

$$(k+1-\delta)(\sqrt{q}+\delta+1) - (k\sqrt{q}+\sqrt{q}+\delta+1) > 0 \ \Leftrightarrow \ \ k > \frac{\delta}{\delta+1}\sqrt{q} + \delta \ .$$

Autrement dit, k est un entier strictement compris entre $\frac{\delta}{\delta+1}\sqrt{q}+\delta$ et $\sqrt{q}$, qui existe dès que

$$\frac{\delta}{\delta+1}\sqrt{q} + \delta + 1 < \sqrt{q} \ \ \Leftrightarrow \ \ (\delta+1)^2 < \sqrt{q}$$

Notons également que si cette dernière inégalité est vérifiée, alors on peut choisir $k = \sqrt{q} - 1 \geq k_{j_0}$, qui est immédiatement vrai dès que $\sqrt{q} > k_{j_0}$. Ainsi, sous la condition que

$$q > q_0 = \max\{(\delta+1)^4; k_{j_0}^2\} \ ,$$

on obtient

$$\frac{\deg(h)}{m} \leq q + (1+2\delta)\sqrt{q} \ \leq q + 2q_0\sqrt{q}$$

et donc

$$\sharp\mathcal{C}(\mathbb{F}_q) \leq q + (2q_0 + \deg(f))\sqrt{q} \ .$$

Si $q_0 \geq q$, on a directement que

$$\sharp\mathcal{C}(\mathbb{F}_q) \leq dq \leq d\sqrt{q_0}\sqrt{q} \leq q + d\sqrt{q_0}\sqrt{q} \ .$$

On peut remarquer que q_0 ne dépend que de d et $\deg(f)$ par construction de la suite (k_j), et on a $q_0 \leq [d{\cdot}\deg(f)]^4$. En posant donc $C = [d{+}\deg(f)][d{\cdot}\deg(f)]^4$, on a pour tout q puissance paire de caractéristique p

$$\sharp\mathcal{C}(\mathbb{F}_q) \leq q + C\sqrt{q} \ .$$

2 GRAPHE DE CAYLEY DANS $\mathbb{F}^*_{q^n}$

Soit f un polynôme unitaire irréductible de $\mathbb{F}_q[X]$. On pose $\deg(f) = n$. On peut donc identifier ainsi $\mathbb{F}_{q^n}$ à $\mathbb{F}_q[\alpha]$, où α est une racine de f. On considère donc le groupe

$$\Gamma_f = \mathbb{F}^*_{q^n} \simeq (\mathbb{F}_q[\alpha])^* \ .$$

Soit $1 \leq d < n$ un entier. On pose

$$I_d = \{\pi \text{ un. ir.} \in \mathbb{F}_q[X]/ \ \deg(g)|d\}$$

$$E_d = \{\pi^{\frac{d}{\deg(\pi)}} / \ \pi \in I_d\}$$

et

$$P_d = \{g(\alpha)/ \ g \in E_d\} \ .$$

On a évidemment $\sharp I_d = \sharp E_d$, mais vu que $d < n$ et tout élement de E_d de degré d, on a aussi $\sharp E_d = \sharp P_d$. Enfin, on remarque que $P_d \subset \mathbb{F}^*_{q^n}$.

Le graphe de Cayley considéré par la suite est le graphe $G(\mathbb{F}^*_{q^n}, P_d)$, où l'ensemble des sommets est le groupe $\mathbb{F}^*_{q^n}$ et l'ensemble des arêtes

$$\{(x, y)/ \ y = \lambda x, \ \lambda \in P_d\} \ .$$

On note ce graphe $G_d(n, q, \alpha)$, car ici $\mathbb{F}^*_{q^n}$ est assimilé à $(\mathbb{F}_q[\alpha])^*$. Avant d'attaquer les propriétés de ce graphe particulier, rappelons que

$$\sum_{g \in E_d} \Lambda(g) = \sum_{\substack{g \text{ un.} \\ \deg(g) = d}} \Lambda(g) = q^d$$

et que

$$\sharp I_d = \sum_{k|d} \iota(k)$$

où $\iota(k)$ est le nombre de polynônes unitaires irréductibles de $\mathbb{F}_q[X]$ de degré k. On rappelle que pour la fonction de Mobius μ,

$$\iota(k) = \frac{1}{k}\sum_{l|k}\mu(l)q^{\frac{k}{l}} \leq \frac{q^k}{k} ,$$

le produit de tous ces polynômes étant un diviseur de $X^{q^k} - X$.

2.1 CONNEXITÉ ET DIAMÈTRE DE $G_d(n, q, \alpha)$

Un graphe de Cayley $\Gamma(G, S)$ est connexe si et seulement si S engendre G. On a donc le premier théorème qui suit:

Théorème 2.1. *On suppose que $n < q^{\frac{d}{2}} + 1$. Alors $G_d(n, q, \alpha)$ est connexe et son diamètre D satisfait à l'inégalité*

$$D \leq 2\frac{n}{d} + 1 + \frac{4\frac{n}{d}\log(n-1)}{d\log(q) - 2\log(n-1)} .$$

Preuve. Supposons par l'absurde que $G_d(n, q, \alpha)$ n'est pas connexe. Alors $< P_d >$ est un sous groupe propre de $(\mathbb{F}_q[\alpha])^*$. On peut donc trouver un caractère non trivial χ tel que $\chi(< P_d >) = 1$. On a par la borne de Weil

$$q^d = \sum_{\substack{g \text{ un.} \\ \deg(g) = d}} \Lambda(g) = | \sum_{\substack{g \text{ un.} \\ \deg(g) = d}} \Lambda(g)\chi(g(\alpha))| \leq (n-1)q^{\frac{d}{2}}$$

et donc que $q^{\frac{d}{2}} + 1 \leq n$ ce qui contredit l'hypothèse de départ. Ainsi, $G_d(n, q, \alpha)$ est connexe.

Pour le calcul du diamètre, on pose pour tout entier $k > 0$ et tout β et Γ_f, $N_k(\beta)$ le nombre de solutions de l'équation

$$\beta = \prod_{i=1}^{k} g_i(\alpha) , \quad g_i \in E_d .$$

On a évidemment que

$$N_k(\beta) = \frac{1}{q^n - 1}\sum_{g_1,\cdots,g_k \in E_d}\sum_{\chi}\chi(\frac{\prod_{i=1}^{k} g_i(\alpha)}{\beta}) .$$

On remarque que $N_k(\beta) > 0$ si et seulement si

$$0 < M_k(\beta) = \frac{1}{q^n - 1}\sum_{g_1,\cdots,g_k \in E_d}\prod_{i=1}^{k}\Lambda(g_i)\sum_{\chi}\chi(\frac{\prod_{i=1}^{k} g_i(\alpha)}{\beta})$$

On a donc

$$\begin{aligned} M_k(\beta) &= \frac{1}{q^n-1}\sum_{g_1,\cdots,g_k\in E_d}\prod_{i=1}^{k}\Lambda(g_i)\sum_{\chi}\chi(\frac{\prod_{i=1}^{k}g_i(\alpha)}{\beta}) \\ &= \frac{1}{q^n-1}\sum_{g_1,\cdots,g_k\in E_d}\sum_{\chi}\chi^{-1}(\beta)\prod_{i=1}^{k}\Lambda(g_i)\chi(g_i(\alpha)) \\ &= \frac{1}{q^n-1}\sum_{\chi}\chi^{-1}(\beta)\sum_{g_1,\cdots,g_k\in E_d}\prod_{i=1}^{k}\Lambda(g_i)\chi(g_i(\alpha)) \\ &= \frac{1}{q^n-1}\sum_{\chi}\chi^{-1}(\beta)[\sum_{g\in E_d}\Lambda(g)\chi(g(\alpha))]^k \ . \end{aligned}$$

Ainsi,

$$M_k(\beta)=\frac{q^{kd}}{q^n-1}+\frac{1}{q^n-1}\sum_{\chi\neq 1}\chi^{-1}(\beta)[\sum_{g\in E_d}\Lambda(g)\chi(g(\alpha))]^k$$

et donc par la borne de Weil

$$M_k(\beta)\geq\frac{q^{kd}}{q^n-1}-\frac{q^n-2}{q^n-1}(n-1)^k q^{\frac{kd}{2}}>\frac{q^{kd}}{q^n-1}-(n-1)^k q^{\frac{kd}{2}} \ .$$

Pour que $M_k(\beta)>0$, il suffit juste que

$$q^{kd}\geq q^n(n-1)^k q^{\frac{kd}{2}} \ \Leftrightarrow \ q^{kd-2n}\geq(n-1)^{2k}$$

Par passage au log, on obtient

$$(kd-2n)\log(q)\geq 2k\log(n-1) \ \Leftrightarrow \ k(d\log(q)-2\log(n-1))\geq 2n\log(q) \ .$$

Or

$$d\log(q)-2\log(n-1)=\log(\frac{q^d}{(n-1)^2})>\log(1)=0$$

par hypothèse. On a donc que dès que

$$k\geq\frac{2n\log(q)}{d\log(q)-2\log(n-1)}=2\frac{n}{d}+\frac{4\frac{n}{d}\log(n-1)}{d\log(q)-2\log(n-1)}$$

$M_k(\beta)>0$ et donc $N_k(\beta)>0$ pour tout β. □

2.2 $G_d(n,q,\alpha)$ COMME GRAPHE EXPANSEUR

On considère la matrice d'adjacence M de $G_d(n,q,\alpha)$ une matrice carré de taille $(q^n-1)\times(q^n-1)$. M agit sur le $\mathbb{C}$-espace vectoriel de dimension q^n-1 des fonctions $\mathbb{C}^{\Gamma_f}$, par

$$M(h)\longmapsto \ x\in\Gamma_f\mapsto\sum_{g\in E_d}h(xg(\alpha)) \ \in\mathbb{C} \ .$$

Pour tout caractère multiplicatif χ de Γ_f, et tout $x \in \Gamma_f$, on a

$$M(\chi)(x) = \sum_{g \in E_d} \chi(xg(\alpha)) = [\sum_{g \in E_d} \chi(g(\alpha))]\chi(x)$$

et donc $M(\chi) = \lambda_d(\chi)\chi$, avec $\lambda_d(\chi) = \sum_{g \in E_d} \chi(g(\alpha))$. χ est donc vecteur propre de M pour la valeur propre $\lambda_d(\chi)$. De plus, par le lemme d'Artin, les $q^n - 1$ caractères de Γ_f sont $\mathbb{C}$-linéairement indépendants. On a donc que les $\lambda_d(\chi)$ sont exactement les valeurs propres de M. On remarque que

$$\lambda_{triv} = \sharp E_d \ .$$

Pour $\chi \neq 1$, on peut majorer $\lambda_d(\chi)$ avec

$$\begin{aligned}
|\lambda_d(\chi)| &= |\sum_{g \in E_d} \chi(g(\alpha))| \\
&= |\sum_{g \in E_d} (\frac{\Lambda(g)}{d} + 1 - \frac{\Lambda(g)}{d})\chi(g(\alpha))| \\
&= |\frac{1}{d}\sum_{g \in E_d} \Lambda(g)\chi(g(\alpha)) + \sum_{g \in E_d} (1 - \frac{\Lambda(g)}{d})\chi(g(\alpha))| \\
&\leq \frac{n-1}{d} q^{\frac{d}{2}} + \sum_{g \in E_d, \Lambda(g) < 1} 1 \\
&\leq \frac{n-1}{d} q^{\frac{d}{2}} + \sum_{k=1}^{d/2} \iota(k) \\
&\leq \frac{n-1}{d} q^{\frac{d}{2}} + \sum_{k=1}^{d/2} \frac{q^k}{k} \\
&\leq \frac{n-1}{d} q^{\frac{d}{2}} + q^{\frac{d}{2}} \ .
\end{aligned}$$

Ainsi, pour tout χ caractère non trivial, on a

$$|\lambda_d(\chi)| \leq \frac{n+d-1}{d} q^{\frac{d}{2}} \ .$$

On remarque que

$$\frac{q^d}{d} = \sum_{g \in E_d} \frac{\Lambda(g)}{d} \leq \sum_{g \in E_d} 1 = \sharp E_d \ .$$

On en déduit directement le théorème suivant :

Théorème 2.2. *Soit $0 < \delta < 1$. On suppose que $(n + d - 1) \leq q^{\frac{d}{2}}(1 - \delta)$. On a donc pour toute valeur propre λ non triviale de la matrice d'adjacence de $G_d(n, q, \alpha)$*

$$|\lambda| \leq \frac{q^d}{d}(1 - \delta) \leq \lambda_{triv}(1 - \delta) \ .$$

En particulier, $G_d(n, q, \alpha)$ est un graphe $\frac{\lambda_{triv}\delta}{2}$-expanseur.

Pour un graphe $G = (X, E)$ donné, et pour toute partie S de X, on note $\Delta(S)$ le nombre d'arêtes reliant S et $X \backslash S$. Et on définit la constante d'expansion $h(G)$ par

$$\min_{S \subset X} \{\frac{\Delta(S)}{\sharp S}\} = \min_{S \subset X, \sharp S \leq \sharp X} \{\frac{\Delta(S)}{\sharp S}\} \ ,$$

puisque $\Delta(S) = \Delta(X \setminus S)$ par définition. On remarque que $h(G) = 0$ si et seulement si G est connexe. On dit d'un graphe qu'il est $\epsilon-$expanseur si $h(G) \geq \epsilon$. Et un théorème nous donne u encadrement plus précis pour des graphes $k-$réguliers connexe, avec

$$\frac{k - \lambda_1}{2} \leq h(G) \leq \sqrt{2k(k - \lambda_1)} \ ,$$

où λ_1 est la deuxième plus grande valeur propre de la matrice d'adjacence de G.

Preuve du thórème. L'inégalité est direct. Le fait que $G_d(n, q, \alpha)$ est un graphe $\frac{\lambda_{triv}\delta}{2}$-expanseur se déduit de

$$h(G) \geq \frac{k - \lambda_1}{2} \geq \frac{\lambda_{triv} - (1 - \delta)\lambda_{triv}}{2} = \frac{\lambda_{triv}\delta}{2}$$

avec k égalant λ_{triv} la plus grande valeur propre et λ_1 la deuxième. □

References

[1] E. Kowalski, **Exponential sums over finite fields, Elementary methods**, Chapitre 4.

[2] DAQING WAN, MATHEMATICS OF COMPUTATION, **Generetors and irreducible polynomials over finite fields**, Volume 66, Numéro 219, Juillet 1997, pages 1195-1212, S0025-5718(97)00835-1

[3] M.Lu, D.Wan, L.-P. Wang, X.-D. Zhang,
Algebraic Cayley graphs over finite fiels, supported by 973 Program(2013CB834203) and National Natural Science Foundation of China 21 Janvier 2014

[4] G. DAVIDOFF, P. SARNAK, A. VALETTE **Elementary number theory, Goup theory and Ramanujan graphs**, Chapitre 1, pages 18-23, 20 janvier 2003