Fonctions zêta : conjectures de Weil et aspects effectifs

Philippe Goutet

exposé donné le 16 novembre 2009

Résumé

Les fonctions zêta sont un moyen de compter les zéros d'un polynôme sur tous les corps finis $\mathbb{F}_{q^r}$ d'un seul coup. Après avoir donné quelques exemples où ce calcul explicite est possible, on rappellera les conjectures de Weil qui décrivent la forme générale des fonctions zêta (en précisant notamment le signe dans l'équation fonctionnelle) et on abordera la question du calcul effectif de la fonction zêta (grâce aux majorations de Bombieri).

Plan

§ 1. Définition et exemples

On considère un nombre premier p et un corps $\mathbb{F}_q$ de caractéristique p. Si f_1, …, f_m sont des polynômes de $\mathbb{F}_q[x_1, \dots, x_n]$, on note X la variété d'équation

$$\begin{cases} f_1(x_1, \dots, x_n) = 0 \\ \dots \\ f_m(x_1, \dots, x_n) = 0 \end{cases}$$

Lorsque $m = 1$, on parle d'hypersurface. Par définition, le nombre de points de X sur $\mathbb{F}_{q^r}$ est le nombre de zéros des polynômes f_1, …, f_m dans $\mathbb{F}_{q^r}^n$ (ou dans $\mathbb{P}^n_{\mathbb{F}_{q^r}}$ si les f_i sont homogènes) ; on le note $|\mathrm{X}(\mathbb{F}_{q^r})|$. La fonction zêta de l'hypersurface X est définie par :

$$\mathrm{Z}_{\mathrm{X}/\mathbb{F}_q}(t) = \exp\left(\sum_{r=1}^{+\infty} |\mathrm{X}(\mathbb{F}_{q^r})| \, \frac{t^r}{r}\right).$$

Elle est simplement reliée à la fonction génératrice du nombre de zéros de f dans les $\mathbb{F}_{q^r}$ par la formule :

$$\frac{\mathrm{Z}'_{\mathrm{X}/\mathbb{F}_q}(t)}{\mathrm{Z}_{\mathrm{X}/\mathbb{F}_q}(t)} = \frac{\mathrm{d}}{\mathrm{d}t}\left(\ln \mathrm{Z}_{\mathrm{X}/\mathbb{F}_q}(t)\right) = \mathrm{G}_{\mathrm{X}/\mathbb{F}_q}(t) \quad \text{où} \quad \mathrm{G}_{\mathrm{X}/\mathbb{F}_q}(t) = \sum_{r=1}^{+\infty} |\mathrm{X}(\mathbb{F}_{q^r})| t^{r-1}.$$

La raison pour laquelle on s'intéresse à la fonction zêta plutôt qu'à la fonction génératrice est que la fonction zêta vérifie un certain nombre de propriétés supplémentaires (conjectures de Weil, aujourd'hui démontrées ; voir § 2).

On commence par deux exemples triviaux (espace affine et espace projectif) puis on donne quatre exemples plus évolués (courbes elliptiques, courbes projectives lisses, grassmanniennes et hypersurfaces diagonales). Pour plus de détails sur l'histoire des conjectures de Weil, on renvoie à [Hou02].

Fonction zêta de l'espace affine. Si on veut rester dans le cadre précédent (fonctions zêta d'une variété donnée par un système d'équations), on peut voir l'espace affine comme l'hypersurface définie par le polynôme identiquement nul et

$$|\mathbb{A}^n_{\mathbb{F}_{q^r}}| = (q^r)^n,$$

d'où

$$\mathrm{Z}_{\mathbb{A}^n_{\mathbb{F}_q}}(t) = \exp\left(\sum_{r=1}^{+\infty} (q^r)^n \frac{t^r}{r}\right) = \exp\left(\sum_{r=1}^{+\infty} \frac{(q^n t)^r}{r}\right) = \exp\Big(-\ln(1-q^n t)\Big) = \frac{1}{1-q^n t}\,.$$

Fonction zêta de l'espace projectif. Rappelons que l'espace projectif $\mathbb{P}^n$ est défini par $\mathbb{P}^n = (\mathbb{A}^{n+1} - \{0\})/\mathbb{F}_q^*$. Avec les notations précédentes, l'espace $\mathbb{P}^{n-1}$ peut être vu comme l'hypersurface d'équation $0 = 0$ (le polynôme étant considéré comme ayant n variables) ; on a

$$|\mathbb{P}^{n-1}(\mathbb{F}_{q^r})| = \frac{(q^r)^n - 1}{q^r - 1} = 1 + q^r + (q^r)^2 + \cdots + (q^r)^{n-1}.$$

Ainsi :

$$\begin{aligned}
\mathrm{Z}_{\mathbb{P}^{n-1}/\mathbb{F}_q}(t) &= \exp\left(\sum_{r=1}^{+\infty} (1 + q^r + (q^r)^2 + \cdots + (q^r)^{n-1})\,\frac{t^r}{r}\right) \\
&= \exp\left(\sum_{r=1}^{+\infty} \frac{t^r}{r}\right) \exp\left(\sum_{r=1}^{+\infty} \frac{(qt)^r}{r}\right) \ldots \exp\left(\sum_{r=1}^{+\infty} \frac{(q^{n-1}t)^r}{r}\right) \\
&= \exp\Big(-\ln(1-t)\Big) \exp\Big(-\ln(1-qt)\Big) \ldots \exp\Big(-\ln(1-q^{n-1}t)\Big) \\
&= \frac{1}{(1-t)(1-qt)\ldots(1-q^{n-1}t)}\,.
\end{aligned}$$

On a l'équation fonctionnelle suivante :

$$\mathrm{Z}_{\mathbb{P}^{n-1}/\mathbb{F}_q}\left(\frac{1}{q^{n-1}t}\right) = (-1)^n q^{\frac{n(n-1)}{2}} t^n \mathrm{Z}_{\mathbb{P}^{n-1}/\mathbb{F}_q}(t).$$

Fonction zêta d'une courbe elliptique. Soit E une courbe elliptique sur $\mathbb{Q}$ (donc une courbe projective lisse), disons donnée en coordonnées affines par une équation explicite $y^2 = x^3 + ax^2 + bx + c$ où $a, b, c \in \mathbb{Q}$. Il existe un nombre fini de nombres premiers p divisant le dénominateur de a, b et c (écrits sous forme irréductible). Cela a donc un sens de considérer E sur $\mathbb{F}_q$ pour une infinité de nombre premier p. Pour une infinité de nombres premiers, $\mathrm{E}/\mathbb{F}_q$ sera lisse.

Pour de tels nombres premiers, Hasse [Has36] a montré en 1936 que la fonction zêta de E était de la forme suivante :

$$\mathrm{Z}_{\mathrm{E}/\mathbb{F}_q}(t) = \frac{1 - a_q t + qt^2}{(1-t)(1-qt)} = \frac{(1-\pi_q t)(1-\overline{\pi}_q t)}{(1-t)(1-qt)}\,,$$

où $\pi_q, \overline{\pi}_q \in \mathbb{C}$ sont des nombres algébriques conjugués de valeur absolue $\sqrt{q}$. En particulier,

$$\Big||\mathrm{E}(\mathbb{F}_q)| - (q+1)\Big| = |a_q| \leq 2\sqrt{q}\,. \qquad \text{(majoration de Hasse-Weil)}$$

Il a récemment été montré que, lorsque $q = p$, ce coefficient a_p était en fait le p-ième coefficient de Fourier d'une forme modulaire de poids 2. On connaît aujourd'hui d'autres exemples de modularité (un exemple parmi beaucoup d'autres : [Sch86, p. 109-110]). Notons pour finir qu'on a l'équation fonctionnelle suivante :

$$\mathrm{Z}_{\mathrm{E}/\mathbb{F}_q}\left(\frac{1}{qt}\right) = \mathrm{Z}_{\mathrm{E}/\mathbb{F}_q}(t).$$

Fonction zêta d'une courbe. Soit $\mathcal{C}$ une courbe projective non singulière de genre g définie sur $\mathbb{F}_q$. Weil a montré en 1940 (voir [Wei40] pour l'annonce et le livre [Wei48] pour une démonstration complète) que la fonction zêta de $\mathcal{C}$ était de la forme :

$$\mathrm{Z}_{\mathcal{C}/\mathbb{F}_q}(t) = \frac{\mathrm{P}(t)}{(1-t)(1-qt)}\,,$$

où le polynôme $\mathrm{P}(t)$ est dans $1 + t\mathbb{Z}[t]$, a pour degré $2g$ et les inverses de ses racines ont pour valeur absolue $\sqrt{q}$. On en déduit la majoration suivante :

$$\Big||\mathcal{C}(\mathbb{F}_q)| - (q+1)\Big| \leq 2g\sqrt{q}\,. \qquad \text{(majoration de Hasse-Weil)}$$

Notons également l'équation fonctionnelle suivante :

$$\mathrm{Z}_{\mathcal{C}/\mathbb{F}_q}\left(\frac{1}{qt}\right) = q^{1-g}t^{2-2g}\mathrm{Z}_{\mathcal{C}/\mathbb{F}_q}(t).$$

Fonction zêta d'une grassmannienne. (D'après [Wei49, p. 508] et [Kol04]) La grassmannienne $\mathrm{G}_{n,k}(\mathbb{F}_q)$ est la variété composée des sous-espaces de dimension k dans l'espaces affine de dimension n. Contrairement aux exemples précédents, on ne peut pas considérer que c'est une hypersurface, mais la fonction zêta se définit de la même manière ; le nombre de points de cette variété est juste le nombre de sous-espaces vectoriels de dimension k dans $\mathbb{F}_q^n$:

$$\begin{aligned}|\mathrm{G}_{n,k}(\mathbb{F}_q)| &= \frac{\text{nombre de familles libres à } k \text{ éléments}}{\text{nombre d'automorphismes d'un espace de dim } k} \\ &= \frac{(q^n-1)(q^n-q)\dots(q^n-q^{k-1})}{(q^k-1)(q^k-q)\dots(q^k-q^{k-1})}\,.\end{aligned}$$

Par exemple :

$$|\mathrm{G}_{4,2}(\mathbb{F}_q)| = \frac{(q^4-1)(q^3-q)}{(q^2-1)(q^2-q)} = (q^2+1)(q^2+q+1) = q^4+q^3+2q^2+q+1,$$

et donc :

$$\mathrm{Z}_{\mathrm{G}_{4,2}(\mathbb{F}_q)/\mathbb{F}_q}(t) = \frac{1}{(1-t)(1-qt)(1-q^2t)^2(1-q^3t)(1-q^4t)}$$

d'où l'équation fonctionnelle

$$\mathrm{Z}_{\mathrm{G}_{4,2}(\mathbb{F}_q)/\mathbb{F}_q}\left(\frac{1}{q^4 t}\right) = q^{12}t^6 \mathrm{Z}_{\mathrm{G}_{4,2}(\mathbb{F}_q)/\mathbb{F}_q}(t).$$

Il n'est pas *a priori* clair que $|\mathrm{G}_{n,k}(\mathbb{F}_q)|$ est toujours un polynôme en q ; pour le montrer, on peut utiliser la relation de récurrence suivante [1]

$$|\mathrm{G}_{n,k}(\mathbb{F}_q)| = |\mathrm{G}_{n-1,k}(\mathbb{F}_q)| + q^{n-k}|\mathrm{G}_{n-1,k-1}(\mathbb{F}_q)|,$$

puis raisonner par récurrence pour obtenir :

$$|\mathrm{G}_{n,k}(\mathbb{F}_q)| = \beta_0 + \beta_1 q + \cdots + \beta_{n(n-k)} q^{n(n-k)}.$$

En fait, le coefficient β_i est égal au nombre de k-uples $0 \leq i_1 \leq \cdots \leq i_k \leq n-k$ tels que $i_1 + \cdots + i_r = i$ (voir [And76, § 3.3 p. 35-34 et § 13.2 p. 212-214]). On a $\beta_i = b_{2i}$, le nombre de Betti de dimension $2i$ de la grassmannienne complexe (calculés par Ehresmann dans [Ehr34, théorème p. 409]). À titre d'exemple, on peut écrire explicitement les partitions correspondant aux différents entiers β_i de $\mathrm{G}_{4,2}(\mathbb{F}_q)$:

COEFICIENTS β_i	$\beta_0 = 1$	$\beta_1 = 1$	$\beta_2 = 2$	$\beta_3 = 1$	$\beta_4 = 1$
PARTITIONS	(0,0)	(0,1)	(0,2),(1,1)	(1,2)	(2,2)

Notons que $\beta_i = \beta_{n(n-k)-i}$.

La fonction zêta de la grassmannienne est donc

$$\mathrm{Z}_{\mathrm{G}_{n,k}(\mathbb{F}_q)/\mathbb{F}_q}(t) = \frac{1}{(1-t)^{\beta_0}(1-qt)^{\beta_1}\dots(1-q^{n(n-k)})^{\beta_{n(n-k)}}}.$$

Posons $\chi = \sum \beta_i$; la fonction zêta de la grassmannienne vérifie l'équation fonctionnelle

$$\mathrm{Z}_{\mathrm{G}_{n,k}(\mathbb{F}_q)/\mathbb{F}_q}\left(\frac{1}{q^{n(n-k)}t}\right) = (-1)^{\chi}(q^{n(n-k)})^{\frac{1}{2}\chi}t^{\chi}\mathrm{Z}_{\mathrm{G}_{n,k}(\mathbb{F}_q)/\mathbb{F}_q}(t).$$

Noter que le signe $(-1)^{\chi}$ est $+1$ si $n(n-k)$ est pair (car $\beta_i = \beta_{n(n-k)-i}$ et donc χ est pair) et est $(-1)^{\beta_{n(n-k)/2}}$ sinon (quantité égale à la multiplicité de $q^{-n(n-k)/2}$ comme racine de $(1 - q^{n(n-k)/2}t)^{\beta_{n(n-k)/2}}$).

Fonction zêta d'une hypersurface diagonale. Dans son célèbre article de 1949 [Wei49] (c'est l'article où il énonce ce que l'on appelle aujourd'hui les conjectures de Weil), Weil détermine la fonction zêta des hypersurfaces diagonales $\mathrm{D}_\alpha : \alpha_1 x_1^d + \cdots + \alpha_n x_n^d = 0$ lorsque $q \equiv 1 \mod d$:

$$\mathrm{Z}_{\mathrm{D}_\alpha/\mathbb{F}_q}(t) = \frac{\prod_{\substack{1\leq s_i\leq d-1 \\ n|s_1+\cdots+s_n}} \left(1 - (-1)^{n-1}\chi^{-s_1}(\alpha_1)\dots\chi^{-s_n}(\alpha_n)\mathrm{J}(\chi^{s_1},\dots,\chi^{s_n})t\right)^{(-1)^{n-1}}}{(1-t)(1-qt)\dots(1-q^{n-2}t)},$$

où $\mathrm{J}(\chi^{s_1},\dots,\chi^{s_n})$ est la somme de Jacobi

$$\mathrm{J}(\chi^{s_1},\dots,\chi^{s_n}) = \sum_{\substack{x_1,\dots,x_n\in\mathbb{F}_q \\ x_1+\cdots+x_n=1}} \chi^{s_1}(x_1)\dots\chi^{s_n}(x_n),$$

1. Pour la démontrer, il suffit d'écrire. Cette relation ressemble fortement à l'identité $\mathrm{C}_n^k = \mathrm{C}_n^{k-1} + \mathrm{C}_{n-1}^{k-1}$ sur les coefficients binomiaux, et ce n'est pas un hasard : les nombres $\mathrm{G}_{n,k}(\mathbb{F}_q)$ sont appelés coefficients q-binomiaux.

le symbole χ désignant un caractère multiplicatif d'ordre d de $\mathbb{F}_q^*$ (prolongé par $\chi(0) = 0$). Une propriété importante des sommes de Jacobi précédentes est que $|\mathrm{J}(\chi^{s_1}, \dots, \chi^{s_n})| = \sqrt{q^{n-2}}$ (le caractère χ étant supposé à valeurs dans $\mathbb{C}$; cette propriété résulte du fait que $\chi^{s_1} \dots \chi^{s_n} = \mathbb{1}$). Si on calcule le degré du numérateur, on trouve $\frac{(d-1)^n+(-1)^n(d-1)}{d}$. Guidé par les exemples précédents, Weil a demandé à Dolbeault de calculer les nombres de Betti de l'hypersurface complexe $\alpha_1 x_1^d + \dots + \alpha_n x_n^d = 0$. Comme on peut s'y attendre, ces nombres sont $b_{n-2} = \frac{(d-1)^n+(-1)^n(d-1)}{d}$ et $b_i = 1$ ou 0 sinon (selon que $i \neq n-2$ est pair ou impair).

§ 2. Conjectures de Weil

Les exemples précédents ont amené Weil à formuler les conjectures suivantes (voir [Wei49]).

Énoncé des conjectures de Weil. Soit X une variété algébrique projective lisse de dimension m définie sur $\mathbb{F}_q$. Il existe (*propriété de Lefschetz*) $2m+1$ polynômes $\mathrm{P}_0, \dots, \mathrm{P}_{2m} \in 1 + t\mathbb{Z}[t]$ tels que :

$$\mathrm{Z}_{\mathrm{X}/\mathbb{F}_q}(t) = \frac{\mathrm{P}_1(t)\mathrm{P}_3(t)\dots\mathrm{P}_{2m-1}(t)}{\mathrm{P}_0(t)\mathrm{P}_2(t)\dots\mathrm{P}_{2d-2}(t)\mathrm{P}_{2m}(t)},$$

où $\mathrm{P}_0(t) = 1 - t$, $\mathrm{P}_{2m}(t) = 1 - q^m t$ et, si on écrit $\mathrm{P}_i(t) = \prod_{j=1}^{b_i}(1 - \alpha_{i,j}t)$ avec $\alpha_{i,j} \in \mathbb{C}$, les $\alpha_{i,j}$ vérifient l'*hypothèse de Riemann* suivante :

$$|\alpha_{i,j}| = q^{\frac{i}{2}}.$$

De plus, si on pose $\chi = \sum_{i=0}^{2m}(-1)^i b_i$ (où $b_i = \deg \mathrm{P}_i$), la fonction zêta vérifie l'*équation fonctionnelle* suivante :

$$\mathrm{Z}_{\mathrm{X}/\mathbb{F}_q}\left(\frac{1}{q^m t}\right) = \varepsilon q^{\frac{m\chi}{2}} t^\chi \mathrm{Z}_{\mathrm{X}/\mathbb{F}_q}(t) \qquad \text{avec} \quad \varepsilon = \begin{cases} +1 & \text{si } m \text{ est impair,} \\ (-1)^{\mathrm{N}} & \text{si } m \text{ est pair et où } (1 - q^{\frac{m}{2}}t)^{\mathrm{N}} \parallel \mathrm{P}_m. \end{cases}$$

Finalement, si X provient d'une variété complexe (par exemple, X est une hypersurface à coefficients entiers), les b_i sont les nombres de Betti de la variété complexe correspondante (et donc χ n'est autre que la caractéristique d'Euler-Poincaré).

Remarques. — La rationalité a été montrée par Dwork en 1960 [Dwo60] pour des variétés quelconques (affines ou projectives, singulières ou non) grâce à des techniques p-adiques ; voir [Kob77, chap. 5]. La propriété de Lefschetz, l'équation fonctionnelle et l'interprétation des nombres de Betti ont été démontrées par Grothendieck et Michael Artin en 1963 ; voir [Gro64, Gro66]. Finalement, Deligne a montré l'hypothèse de Riemann en 1974 ; voir [Del74].

Cas d'une hypersurface. Dans le cas d'une hypersurface projective non singulière, on peut préciser un peu les conjectures de Weil. Soit X l'hypersurface de $\mathbb{P}^{n-1}$ définie par l'équation $f = 0$ avec $f \in \mathbb{F}_q[x_1, \dots, x_n]$ homogène de degré d et non singulier ; la dimension de X est $m = n - 2$. Dans ces conditions, Dwork [Dwo62, Dwo64] a montré qu'il existait un polynôme $\mathrm{P}(t) \in 1 + t\mathbb{Z}[t]$ de degré $\frac{(d-1)^n+(-1)^n(d-1)}{d}$ tel que :

$$\mathrm{Z}_{\mathrm{X}/\mathbb{F}_q}(t) = \frac{\mathrm{P}(t)^{(-1)^{n-1}}}{(1-t)(1-qt)\dots(1-q^{n-2}t)}.$$

L'hypothèse de Riemann permet de montrer que les inverses des racines de P sont toutes de valeur absolue $q^{\frac{n-2}{2}}$.

§ 3. Aspects algorithmiques

Tout ce § 3 est basé sur l'article [Wan03], qui présente des arguments de Lenstra, parfaitement élémentaires, pour calculer effectivement la fonction zêta à partir des nombres de points. On commence par des rappels sur le degré total d'une fraction rationnelle.

Notion de degré total d'une fraction rationnelle. Soit $F \in \mathbb{K}(X)$. On écrit $F = P/Q$ avec $P, Q \in \mathbb{K}[X]$ premiers entre eux et on pose :

$$\deg \mathrm{tot}(F) = \deg P + \deg Q.$$

C'est le nombre de racines et de pôles de F, comptés avec multiplicité.

Noter que, par définition même,

$$\deg \mathrm{tot}\left(\frac{1}{F}\right) = \deg \mathrm{tot}\, F$$

et, si $F_1 = P_1/Q_1$ et $F_2 = P_2/Q_2$ sont deux éléments de $\mathbb{K}(X)$ écrits sous forme irréductible, on a :

$$F_1F_2 = \frac{P_1P_2}{Q_1Q_2} \quad \text{et donc} \quad \deg \mathrm{tot}(F_1F_2) \leq \deg \mathrm{tot}(F_1) + \deg \mathrm{tot}(F_2).$$

3.1. Présentation de l'algorithme

Tout ce n° est basé sur [Wan03, cor 2.7, p. 7-8].

Noter que si on connaît le signe dans l'équation fonctionnelle de la fonction zêta (par exemple, en dimension impaire pour une variété projective lisse), on a seulement besoin de calculer la moitié des coefficients de la fonction zêta.

Numérateur et dénominateur des fonctions zêta. Rappelons qu'on considère une variété X donnée par un système

$$\begin{cases} f_1(x_1, \ldots, x_n) = 0 \\ \ldots \\ f_m(x_1, \ldots, x_n) = 0 \end{cases}$$

et qu'on ne fait aucune hypothèse sur les polynômes f_i (notamment, X peut être singulière). Si on écrit $Z_{X/\mathbb{F}_q}(t) = A/B$ avec $A, B \in 1 + t\mathbb{Q}[t]$ premiers entre eux, notre but est de calculer A et B. On a besoin pour cela de savoir jusqu'à quel rang on doit calculer les $|X(\mathbb{F}_{q^r})|$ et pour cela, il faut majorer $\deg A$ et $\deg B$. On notera ces majorants α et β. Si on connaît les degrés de A et B (c'est le cas si par exemple X est une hypersurface lisse : $\deg A = \frac{(d-1)^n+(-1)^n(d-1)}{d}$ et $\deg B = n - 1$ où $d = \deg f_1$), on utilisera bien sûr ces majorants-là (qui sont optimaux). Si on ne connaît pas leurs degrés (et qu'on ne peut pas majorer les nombres de Betti), on remarquera que $\deg A$ et $\deg B$ sont majorés par $\deg \mathrm{tot}\, Z_{X/\mathbb{F}_q}(t)$ et on utilisera l'une des deux majorations

suivantes (basées sur la majoration de Bombieri, voir n° sec:majorationbombieri pour plus de précision) :

$$\deg \mathrm{tot}\, Z_{X/\mathbb{F}_q}(t) \leq (4d+9)^{n+m} \qquad \text{(méthode directe)}$$

$$\deg \mathrm{tot}\, Z_{X/\mathbb{F}_q}(t) \leq (2^m-1)(4d'+9)^{n+1} \qquad \text{(méthode de dichotomie)}$$

où $d = \max \deg f_i$ et $d' = \sum \deg f_i$.

Premier termes de la fonction zêta. Ensuite, on calcule les $|X(\mathbb{F}_{q^r})|$ pour $1 \leq r \leq \alpha+\beta$ (ce calcul est algorithmique, quitte à utiliser un comptage exhaustif), ce qui fournit les $\alpha+\beta+1$ premiers termes de la fonction zêta (en tronquant l'exponentielle) sous forme d'un polynôme

$$Z_{\alpha+\beta} = 1 + z_1 t + z_2 t^2 + \cdots + z_{\alpha+\beta} t^{\alpha+\beta}.$$

Système linéaire. Une fois ces premiers termes calculés, on écrit :

$$A(t) = 1 + a_1 t + \ldots + a_\alpha t^\alpha \quad \text{et} \quad B(t) = 1 + b_1 t + \ldots + b_\beta t^\beta.$$

La congruence $B(t)Z_{\alpha+\beta}(t) \equiv A(t) \mod t^{\alpha+\beta+1}$ fournit alors un système linéaire de $\alpha+\beta$ équations en les $\alpha+\beta$ variables $(a_1, \ldots, a_\alpha, b_1, \ldots, b_\beta)$. Puisque l'on sait, par rationalité de la fonction zêta, que cette équation a au moins une solution dans $\mathbb{Q}^{\alpha+\beta}$, on peut en trouver une en résolvant le système (algèbre linéaire élémentaire). Notons cette solution $(\tilde{a}_1, \ldots, \tilde{a}_\alpha, \tilde{b}_1, \ldots, \tilde{b}_\beta)$ et posons :

$$\tilde{A}(t) = 1 + \tilde{a}_1 t + \ldots + \tilde{a}_\alpha t^\alpha \quad \text{et} \quad \tilde{B}(t) = 1 + \tilde{b}_1 t + \ldots + \tilde{b}_\beta t^\beta.$$

Simplification du résultat. Les polynomes $\tilde{A}$ et $\tilde{B}$ ne sont pas nécessairement les polynômes A et B que l'on cherche. Pour s'y ramener, on remarque que, par définition même, $\tilde{B}(t)Z_{\alpha+\beta}(t) \equiv \tilde{A}(t) \mod T^{\alpha+\beta+1}$ et donc :

$$B(t)\tilde{A}(t) \equiv B(t)\tilde{B}(t)Z_{\alpha+\beta}(t) \equiv \tilde{B}(t)A(t) \mod T^{\alpha+\beta+1},$$

d'où $B(t)\tilde{A}(t) = \tilde{B}(t)A(t)$ puisque ces deux polynômes sont de degré $\leq \alpha+\beta$. Par suite, on a $Z_X(t) = \frac{A(t)}{B(t)} = \frac{\tilde{A}(t)}{\tilde{B}(t)}$. En simplifiant $\tilde{A}(t)$ et $\tilde{B}(t)$ par leur PGCD (ce qui est parfaitement algorithmique), on obtient ainsi $A(t)$ et $B(t)$ (qui sont premiers entre eux) et donc la fonction zêta.

Traduction en Maple de l'algorithme précédent. La procédure Maple suivante prend en entrée le majorant α du numérateur de la fonction zêta, le majorant β du dénominateur de la fonction zêta, ainsi que la liste des $\alpha+\beta+1$ premiers zéros et renvoie la fonction zêta. L'algorithme est rapide, même pour une fonction zêta relativement grande, une fois que les zéros ont été calculés.

```
interpolzeta:=proc(alpha,beta,zeros)
  local A,B,EXPO,z,Z,P,S,i,t,T;
  A:=1; for i from 1 to alpha do A:=A+a[i]*t^i od;
  B:=1; for i from 1 to beta do B:=B+b[i]*t^i od;
  EXPO:=0; for i from 1 to alpha+beta do EXPO:=EXPO+zeros[i]*t^i/i; od;
  z:=series(exp(EXPO),t=0,alpha+beta+1);
```

```
  Z:=0; for i from 0 to alpha+beta do Z:=Z+coeff(z,t,i)*t^i; od;
  P:=collect(A-B*Z,t);
  S:={seq(coeff(P,t,i)=0,i=0..alpha+beta)};
  T:=solve(S);
  subs(T,A)/subs(T,B);
end;
```

Remarque sur l'efficacité de l'algorithme. L'étape la plus coûteuse de l'algorithme précédent est le calcul des $|\mathrm{X}(\mathbb{F}_{q^r})|$ pour $1 \leq r \leq \alpha+\beta$, surtout si on utilise la méthode de comptage exhaustif. Cela veut dire qu'en pratique l'algorithme est inutilisable si on n'a pas une méthode plus efficace (par exemple, on a pu calculer le nombre de points de X en terme de sommes de Gauss ; il sera alors plus efficace d'exprimer (via la formule de Gross-Koblitz) ces sommes de Gauss grâce à la fonction Gamma p-adique qui se calcule très bien ; voir [Wan03, p. 8-9] pour un certain nombre d'algorithmes modernes sur le sujet). Les autres étapes de l'algorithme précédent sont relativement peu coûteuse : tronquer l'exponentielle d'un développement limité jusqu'au terme $\alpha+\beta+1$, résoudre un système linéaire de taille $\alpha+\beta$ et calculer un PGCD dans $\mathbb{Q}[t]$ entre deux polynômes de degrés α et β.

Ensuite, une fois la fonction zêta calculée, on peut se demander quelle est l'efficacité de calculer un $|\mathrm{X}(\mathbb{F}_{q^r})|$ pour r très grand ; en fait, le temps est linéaire en r (car les coefficients d'une série qui est une fraction rationnelle vérifient, à partir d'un certain rang, une équation de récurrence linéaire).

3.2. Majoration de Bombieri

On présente ici la majoration montrée par Bombieri dans [Bom78, thm 1, p. 30]. Son théorème est le suivant.

Théorème 1. — *Soit* $\mathrm{P} \in \mathbb{F}_q[x_1, \dots, x_n]$ *un polynôme de degré* d *et* φ *un caractère additif non trivial de* $\mathbb{F}_q$ *à valeurs dans un certain corps algébriquement clos* Ω *de caractéristique nulle. On pose :*

$$\mathrm{S}_r(\mathrm{P}) = \sum_{x \in \mathbb{F}_{q^r}} (\varphi \circ \mathrm{Tr}_{\mathbb{F}_{q^r}/\mathbb{F}_q})(\mathrm{P}(x)) \quad \textit{et} \quad \mathrm{L}_\mathrm{P}(t) = \exp\left(\sum_{r=1}^{+\infty} \mathrm{S}_r(\mathrm{P})\,\frac{t^r}{r}\right).$$

Il est connu que la fonction L_P *appartient à* $\Omega(t)$ *et on a la majoration*

$$\deg \mathrm{tot}\, \mathrm{L}_\mathrm{P} \leq (4d+5)^n.$$

Il reste deux problèmes : expliquer en quoi ce résultat est relié aux fonctions zêta et comment étendre la majoration au cas de plusieurs polynômes (il y aura deux méthodes, chacune aboutissant à un résultat meilleur dans certains cas de figures).

Pour le premier point, il s'agit d'exprimer le nombre de zéros en terme de sommes du type $\mathrm{S}_r(\mathrm{P})$.

Proposition 2. — *Si* X *est la variété affine d'équations* $f_1 = \cdots = f_m = 0$ *et si* $d = \max \deg f_i$, *alors, si* $\mathrm{P} = a_1 f_1 + \cdots + a_m f_m$, *on a*

$$\mathrm{Z}_{\mathrm{X}/\mathbb{F}_q}(t) = \mathrm{L}_\mathrm{P}(t/q^m) \quad \textit{et donc} \quad \deg \mathrm{tot}\, \mathrm{Z}_{\mathrm{X}/\mathbb{F}_q}(t) \leq (4d+9)^{n+m}.$$

Démonstration. Rappelons la formule d'orthogonalité suivante. Si φ est un caractère non trivial (c'est-à-dire non constant égal à 1), alors tous les autres caractères de $\mathbb{F}_q$ sont de la forme $x \mapsto \varphi(ax)$ pour $a \in \mathbb{F}_q$ et tous les caractères de $\mathbb{F}_{q^r}$ sont de la forme $x \mapsto (\varphi \circ \mathrm{Tr}_{\mathbb{F}_{q^r}/\mathbb{F}_q})(ax)$ et on a

$$\forall y \in \mathbb{F}_{q^r}, \quad \sum_{a \in \mathbb{F}_{q^r}} (\varphi \circ \mathrm{Tr}_{\mathbb{F}_{q^r}/\mathbb{F}_q})(ay) = \begin{cases} q^r & \text{si } y = 0, \\ 0 & \text{si } y \neq 0. \end{cases}$$

Si $f \in \mathbb{F}_q[\mathrm{X}_1, \ldots, \mathrm{X}_n]$, on peut donc écrire :

$$|\{x \in \mathbb{F}_{q^r}^n\} f(x) = 0| = \frac{1}{q^r} \sum_{a \in \mathbb{F}_{q^r}} \sum_{x \in \mathbb{F}_{q^r}^n} (\varphi \circ \mathrm{Tr}_{\mathbb{F}_{q^r}/\mathbb{F}_q})(af(x)).$$

Plus généralement,

$$\begin{aligned}
|\mathrm{X}(\mathbb{F}_{q^r})| &= |\{x \in \mathbb{F}_{q^r}^n\} f_1(x) = \ldots = f_m(x) = 0| \\
&= \left(\frac{1}{q^r} \sum_{a_1 \in \mathbb{F}_{q^r}} \varphi(\mathrm{Tr}_{\mathbb{F}_{q^r}/\mathbb{F}_q}(a_1 f_1(x))) \right) \ldots \left(\frac{1}{q^r} \sum_{a_m \in \mathbb{F}_{q^r}} \varphi(\mathrm{Tr}_{\mathbb{F}_{q^r}/\mathbb{F}_q}(a_m f_m(x))) \right) \\
&= \frac{1}{q^{mr}} \sum_{a \in \mathbb{F}_{q^r}^m} \sum_{x \in \mathbb{F}_{q^r}^n} \varphi(\mathrm{Tr}_{\mathbb{F}_{q^r}/\mathbb{F}_q}(a_1 f_1(x))) \varphi(\mathrm{Tr}_{\mathbb{F}_{q^r}/\mathbb{F}_q}(a_2 f_2(x))) \ldots \varphi(\mathrm{Tr}_{\mathbb{F}_{q^r}/\mathbb{F}_q}(a_m f_m(x))) \\
&= \frac{1}{q^{mr}} \sum_{a \in \mathbb{F}_{q^r}^m} \sum_{x \in \mathbb{F}_{q^r}^n} \varphi(\mathrm{Tr}_{\mathbb{F}_{q^r}/\mathbb{F}_q}((a_1 f_1 + \ldots + a_m f_m)(x))) \\
&= \frac{1}{q^{mr}} \sum_{a \in \mathbb{F}_{q^r}^m, x \in \mathbb{F}_{q^r}^n} \varphi(\mathrm{Tr}_{\mathbb{F}_{q^r}/\mathbb{F}_q}(\mathrm{P}(x)))
\end{aligned}$$

avec $\mathrm{P} = \mathrm{A}_1 f_1 + \ldots + \mathrm{A}_m f_m \in \mathbb{F}_q[\mathrm{A}_1, \ldots, \mathrm{A}_m, \mathrm{X}_1, \ldots, \mathrm{X}_n]$ de degré $\max(\deg f_i) + 1 = d + 1$ à $n + m$ variables. On a donc

$$\mathrm{Z}_{\mathrm{X}/\mathbb{F}_q}(t) = \mathrm{L}_{\mathrm{P}}(t/q^m) \quad \text{d'où} \quad \deg \mathrm{tot}\, \mathrm{Z}_{\mathrm{X}/\mathbb{F}_q}(t) \leq (4(d+1)+5)^{n+m} = (4d+9)^{n+m}. \qquad \square$$

Proposition 3. — *Si* X *est la variété affine d'équations* $f_1 = \cdots = f_m = 0$ *et si* $d' = \sum \deg f_i$, *alors, en notant* H_{I} *l'hypersurface affine d'équation* $\prod_{i \in \mathrm{I}} f_i = 0$ *pour* $\mathrm{I} \subset \{1, \ldots, m\}$,

$$\mathrm{Z}_{\mathrm{X}/\mathbb{F}_q}(t) = \prod_{\substack{\mathrm{I} \subset \{1,\ldots,m\} \\ \mathrm{I} \neq \varnothing}} \mathrm{Z}_{\mathrm{H}_{\mathrm{I}}/\mathbb{F}_q}(t)^{(-1)^{|\mathrm{I}|+1}} \quad \textit{et donc} \quad \deg \mathrm{tot}\, \mathrm{Z}_{\mathrm{X}/\mathbb{F}_q}(t) \leq (2^m - 1)(4d' + 9)^{n+1}.$$

Démonstration. On démontre d'abord la formule sur la fonction zêta de X puis on utilise la proposition précédente pour majorer tous les degré totaux de $\mathrm{Z}_{\mathrm{H}_{\mathrm{I}}/\mathbb{F}_q}(t)$.

Le principe est le suivant. Si $m = 2$, on a

$$|\mathrm{X}| = |\mathrm{H}_{\{1\}}| + |\mathrm{H}_{\{2\}}| - |\mathrm{H}_{\{1,2\}}|,$$

et si $m = 3$, on a

$$|\mathrm{X}| = |\mathrm{H}_{\{1\}}| + |\mathrm{H}_{\{2\}}| + |\mathrm{H}_{\{3\}}| - |\mathrm{H}_{\{1,2\}}| - |\mathrm{H}_{\{1,3\}}| - |\mathrm{H}_{\{2,3\}}| + |\mathrm{H}_{\{1,2,3\}}|,$$

et plus généralement, pour m quelconque,

$$|\mathrm{X}| = \sum_{\substack{\mathrm{I}\subset\{1,\dots,m\}\\ \mathrm{I}\neq\varnothing}} (-1)^{|\mathrm{I}|+1}\mathrm{H}_\mathrm{I}, \quad \text{d'où} \quad \mathrm{Z}_{\mathrm{X}/\mathbb{F}_q}(t) = \prod_{\substack{\mathrm{I}\subset\{1,\dots,m\}\\ \mathrm{I}\neq\varnothing}} \mathrm{Z}_{\mathrm{H}_\mathrm{I}/\mathbb{F}_q}(t)^{(-1)^{|\mathrm{I}|+1}}.$$

Il y a $2^m - 1$ facteurs dans ce produit.

En appliquant les propriétés du degré total rappelées plus haut (page 6) à la formule pour les fonctions zêta que l'on vient juste d'obtenir, on a :

$$\deg \mathrm{tot}\, \mathrm{Z}_{\mathrm{X}/\mathbb{F}_q}(t) \leq \sum_{\substack{\mathrm{I}\subset\{1,\dots,m\}\\ \mathrm{I}\neq\varnothing}} \deg \mathrm{tot}(\mathrm{Z}_{\mathrm{H}_\mathrm{I}}(t)),$$

avec, d'après la majoration de Bombieri appliquée à l'hypersurface H_I,

$$\deg \mathrm{tot}\, \mathrm{Z}_{\mathrm{H}_\mathrm{I}/\mathbb{F}_q}(t) \leq \left(4 \deg\left(\prod_{i\in\mathrm{I}} f_i\right) + 9\right)^{n+1} \leq \left(4\sum_{i\in\mathrm{I}} \deg f_i + 9\right)^{n+1}.$$

Par suite :

$$\deg \mathrm{tot}\, \mathrm{Z}_{\mathrm{X}/\mathbb{F}_q}(t) \leq \sum_{\substack{\mathrm{I}\subset\{1,\dots,m\}\\ \mathrm{I}\neq\varnothing}} \left(4\sum_{i\in\mathrm{I}} \deg f_i + 9\right)^{n+1}.$$

On peut bien sûr majorer les sommes sur les degrés de f_i par $d' = \deg f_1 + \cdots + \deg f_m$, ce qui donne

$$\deg \mathrm{tot}\, \mathrm{Z}_{\mathrm{X}/\mathbb{F}_q}(t) \leq (2^m - 1)(4d' + 9)^{n+1},$$

mais la majoration devient moins bonne (et chaque unité compte dans la majoration vu les temps de calcul en jeu). □

Références

[And76] Andews (George E.) – *The Theory of Partitions*, addison-wesley éd., Encyclopedia of Mathematics and its Applications, vol. 2, 1976.

[Bom78] Bombieri (Enrico) – « On exponential sums in finite fields, II », *Invent. Math.* **47** (1978), p. 29-39, disponible sur : `http://www-gdz.sub.uni-goettingen.de/cgi-bin/digbib.cgi?PPN356556735_0047`.

[Del74] Deligne (Pierre) – « La conjecture de Weil : I », *Pub. Math. IHES* **43** (1974), p. 273-307, disponible sur : `http://www.numdam.org/item?id=PMIHES_1974__43__273_0`.

[Del80] ——— , « La conjecture de Weil : II », *Pub. Math. IHES* **52** (1980), p. 137-252, disponible sur : `http://www.numdam.org/item?id=PMIHES_1980__52__137_0`.

[Dwo60] Dwork (Bernard M.) – « On the rationnality of the zeta function of an algebraic variety », *Amer. J. Math.* **82** (1960), p. 631-648.

[Dwo62] ——— , « On the zeta function of a hypersurface I », *Pub. Math. IHES* **12** (1962), p. 5-68, disponible sur : `http://www.numdam.org/item?id=PMIHES_1962__12__5_0`.

[Dwo64] ——— , « On the zeta function of a hypersurface II », *Ann. of Math.* **80** (1964), p. 227-299.

[Ehr34] Ehresmann (Charles) – « Sur la topologie de certains espaces homogènes », *Ann. of Math.* **35** (1934), no. 2, p. 396-443.

[Gro64] Grothendieck (Alexandre) (éd.) – *Théorie des topos et cohomologie étale des Schémas (SGA 4)*, Springer, 1963-64, Lecture notes in mathematics, vol. 269, 270 et 305, Séminaire de Géométrie Algébrique du Bois-Marie, disponible sur : http://modular.fas.harvard.edu/sga/sga/pdf/index.html.

[Gro66] ——— (éd.) – *Cohomologie ℓ-adique et fonction* L *(SGA5)*, 1965-66, Lecture notes in mathematics, vol. 589, Séminaire de Géométrie Algébrique du Bois-Marie, disponible sur : http://modular.fas.harvard.edu/sga/sga5/index.html.

[Has36] Hasse (Helmut) – « Ueber die Riemannsche Vermuntung im Funktionenkörpern », *Congrès international d'Oslo* (1936).

[Hou02] Houzel (Christian) – « La géométrie algébrique – Recherches historiques », ch. XIII, Albert Blanchard, Paris, 2002.

[Kob77] Koblitz (Neal) – *p-adic Numbers, p-adic Analysis, and Zeta-Functions*, second edition éd., GTM, vol. 58, Springer, Berlin, 1977.

[Kol04] Kolhatkar (Ratnadha) – « Zeta function of Grassmann Varieties », http://www.math.mcgill.ca/goren/SeminarOnCohomology/GrassmannVarieties%20.pdf, 2004.

[Sch86] Schoen (Chad) – « On the geometry of a special determinantal hypersurface associated to the Mumford-Horrocks vector bundle », *J. Reine Angew. Math.* **364** (1986), p. 85-111, disponible sur : http://www-gdz.sub.uni-goettingen.de/cgi-bin/digbib.cgi?PPN243919689_0364.

[Wan03] Wan (Daqing) – « Algorithmic theory of zeta functions over finite fields », *MSRI* (2003), preprint, disponible sur : http://www.math.uci.edu/~dwan/azeta.ps.

[Wei40] Weil (André) – « Sur les fonctions algébriques à corps de constantes fini », *Comptes rendus de l'Académie des Sciences de Paris* **210** (1940), p. 592-594.

[Wei48] ——— , *Sur les courbes algébriques et les variétés qui s'en déduisent*, Actualités scientifiques et industrielles, vol. 1041, Hermann, 1948.

[Wei49] ——— , « Numbers of solutions of equations in finite fields », *Bull. Amer. Math. Soc.* **55** (1949), p. 497-508, disponible sur : http://berndt-schwerdtfeger.de/v4/nf.pdf.