DISTINCTION DE REPRÉSENTATIONS AUTOMORPHES À L'AIDE D'UN NOMBRE MINIMAL D'OPÉRATEURS DE HECKE

THOMAS MÉGARBANÉ

1. Introduction

Dans un précédent travail [14], l'auteur a calculé des traces du paramètre de Satake en p de certaines représentations automorphes algébriques régulières autoduales des groupes linéaires découvertes par Chenevier–Renard [2]. Pour des raisons d'ordre algorithmique liées au temps de calcul, les résultats ont été explicités jusqu'à $p = 67$ dans le meilleur des cas. S'est alors posée la question de savoir jusqu'à quelle valeur de p il était nécessaire d'aller pour déterminer sans ambiguïté les représentations automorphes considérées. L'objectif de cet article est de donner une borne explicite pour la valeur de p jusqu'à laquelle il faudrait calculer des opérateurs de Hecke (ou, de manière équivalente, des traces de paramètre de Satake).

Notre point de départ est un résultat de Deligne [6, Lemme 2.6], qui nous donne pour les formes automorphes sur les corps de fonctions un résultat analogue à celui espéré pour les corps de nombres. On explique plus en détail cette situation au paragraphe 2. Pour les corps de nombres, c'est un résultat d'Iwaniec–Kowalski [10] (en admettant GRH) qui nous permet d'avoir une borne convenable. Leur résultat s'exprime en termes de "fonctions L", comme on l'explique au paragraphe 3. Suivant les résultats récents d'Euvrard [9], on a une borne explicite, malheureusement bien plus grande que les valeurs pour lesquelles des paramètres de Satake ont été calculés dans [14].

Les résultats évoqués ci-dessous donnent, selon les situations, une borne suffisante sur le nombre d'opérateurs de Hecke à calculer pour déterminer complètement une forme automorphe. Le paragraphe 4 s'intéresse à l'optimalité de cette borne. À travers certains exemples, aussi bien dans le cas des corps de fonctions que dans celui des corps de nombres, on compare la borne trouvée à une "borne optimale théorique", dont la valeur repose uniquement sur la dimension des espaces de formes automorphes considérés. Les bornes effectives des paragraphes 2 et 3 apparaissent alors satisfaisantes, puisqu'elles ont des formes très proches de ces bornes théoriques.

On peut en dire un peu plus dans le cas des corps de nombres, qui est le cas qui nous intéressait initialement. Nos calculs de bornes théoriques se limitent aux représentations de PGL_2, qui proviennent de formes modulaires classiques de poids k et de niveau N, et qu'il est donc possible de compter. Lorsque l'on fait varier N, en fixant k, la borne explicite de notre théorème n'est satisfaisante que du point de vue asymptotique, du fait de la grande valeur de la constante explicitée par Euvrard. Lorsque l'on fait varier k, en fixant N, on préfèrera utiliser un résutlat de Sturm [16]. La borne théorique que l'on calcule alors va dans le sens d'une conjecture de Chow–Ghitza [3], déjà évoquée dans les travaux d'Euvrard.

La partie sur les corps de fonctions doit beaucoup à Vincent Lafforgue, qui a aussi contribué plus globalement à cet article par ses nombreuses remarques pertinentes. L'auteur remercie aussi Aurel Page pour avoir signalé le résultat d'Iwaniec–Kowalski [10], ainsi qu'Emmanuel Kowalski pour avoir signalé les travaux d'Euvrard [9].

2. Le cas des corps de fonctions

2.1. Rappels et notations. Commençons par quelques rappels, suivant [13].

Soient $\mathbb{F}_q$ un corps fini, de caractéristique p, de clôture algébrique $\overline{\mathbb{F}_q}$, et ℓ un nombre premier différent de p.

Soit X une courbe projective lisse, géométriquement irréductible sur $\mathbb{F}_q$.

Soient S un ensemble fini de places de X et $U = X \setminus S$.

Soient $\mathcal{F}$ un $\overline{\mathbb{Q}_\ell}$-faisceau lisse sur U, et $\mathcal{K} = j_*\mathcal{F}$ (au sens des faisceaux), où $j : U \to X$ désigne l'inclusion. On note que $\mathcal{K}$ est aussi un faisceau pervers.

Pour tout $s \in S$, on note $Sw_s(\mathcal{F}) \in \mathbb{N}$ le conducteur de Swan de $\mathcal{F}$ en s, qui est nul si, et seulement si, $\mathcal{F}$ est modérément ramifié en s.

On note r le rang de $\mathcal{F}$, et pour tout $s \in S$ on note

$$r_s(\mathcal{F}) = \dim_{\overline{\mathbb{Q}_\ell}}(\mathcal{K}_{\overline{s}}) = \dim_{\overline{\mathbb{Q}_\ell}}\left((\mathcal{F}_{\overline{\eta_s}})^{I_s}\right)$$

où $\overline{s}$ est un point géométrique au-dessus de s, $\overline{\eta_s}$ est un point géométrique générique sur le trait hensélien en s, et I_s est le groupe d'inertie en s.

On note alors $a_s(\mathcal{F}) = (r - r_s(\mathcal{F})) + Sw_s(\mathcal{F}) \in \mathbb{N}$ la chute totale du rang en s (aussi appelé conducteur d'Artin), qui s'annule si, et seulement si, $\mathcal{F}$ s'étend en un faisceau lisse en s.

On note $X_{\overline{\mathbb{F}_q}} = X \underset{\operatorname{Spec}\mathbb{F}_q}{\times} \operatorname{Spec}\overline{\mathbb{F}_q}$.

D'après la formule de Grothendieck–Ogg–Shafarevich, la caractéristique d'Euler–Poincaré de $X_{\overline{\mathbb{F}_q}}$ est égale à :

$$\chi(X_{\overline{\mathbb{F}_q}}, \mathcal{K}) = r\,\chi(X_{\overline{\mathbb{F}_q}}, \overline{\mathbb{Q}_\ell}) - \sum_{s\in S} \deg(s) a_s(\mathcal{F}).$$

On a bien sûr $\chi(X_{\overline{\mathbb{F}_q}}, \overline{\mathbb{Q}_\ell}) = 2 - 2g$, en notant g le genre de X.

En général, pour tout $K \in D^b_c(X, \overline{\mathbb{Q}_\ell})$, on pose :

$$L(X, K, t) = \prod_{x\in|X|} \frac{1}{\det\left(1 - t^{\deg(x)}\operatorname{Frob}_x, K_{\overline{x}}\right)}$$

qui vérifie l'égalité :

$$L(X, K, t) = \det\left(1 - t\operatorname{Frob}_q, R\Gamma\left(X_{\overline{\mathbb{F}_q}}, K\right)\right)^{-1}.$$

En notant $D(K)$ le dual de K, on a une dualité parfaite :

$$R\Gamma(X_{\overline{\mathbb{F}_q}}, K) \otimes R\Gamma(X_{\overline{\mathbb{F}_q}}, D(K)) \to \overline{\mathbb{Q}_\ell}.$$

On en déduit l'égalité :

$$L(X, K, T) = \varepsilon(X, K) t^{a(X,K)} L(X, D(K), t^{-1})$$

où $a(X, K) = -\chi(X_{\overline{\mathbb{F}_q}}, K)$ et $\varepsilon(X, K) = \det(-\operatorname{Frob}_q, R\Gamma(X_{\overline{\mathbb{F}_q}}, K))^{-1}$.

On revient à $K = \mathcal{K} = j_*\mathcal{F}$, avec $j : U \to X$ et $\mathcal{F}$ lisse sur U. On a alors $D(\mathcal{K}) = j_*\mathcal{F}^\vee[2](1)$, où $\mathcal{F}^\vee = \operatorname{Hom}(\mathcal{F}, \overline{\mathbb{Q}_\ell})$ est le dual de $\mathcal{F}$ sur U.

En faisant l'abus de notation $L(X, \mathcal{F}, t)$ (respectivement $\varepsilon(X, \mathcal{F})$, $(a(X, \mathcal{F}))$ au lieu de $L(X, \mathcal{K}, t)$ (respectivement $\varepsilon(X, \mathcal{K})$, $(a(X, \mathcal{K}))$, on a l'égalité :

$$L(X, \mathcal{F}, t) = \varepsilon(X, \mathcal{F}) t^{a(X,\mathcal{F})} L(X, \mathcal{F}^\vee, q^{-1}t^{-1}).$$

Enfin, suivant les notations précédentes, on a : $a(X, \mathcal{F}) = r(2g - 2) + \sum_{s\in S} \deg s \cdot a_s(\mathcal{F})$.

Finissons ce paragraphe en rappelant un résultat de [5]. Étant donné $\iota : \overline{\mathbb{Q}_\ell} \simeq \mathbb{C}$, si $\mathcal{F}$ est un faisceau lisse et ι-pur de poids w sur U, alors pour tout i, $\mathrm{H}^i(X_{\overline{\mathbb{F}_q}}, j_*\mathcal{F})$ est ι-pur de poids $w+i$.

2.2. **Un lemme de Deligne.** L'objectif de ce paragraphe est de donner une variante de [6, Lemme 2.6] (qui apparaît aussi dans [8, Lemme 5.3]).

Soient $\mathcal{F}, \mathcal{G}$ deux $\mathbb{Q}_\ell$-faisceaux lisses sur $U \subset X$.

On rappelle déjà que, d'après [8, 3.2] par exemple, pour tout $s \in S$ on a l'inégalité :

$$Sw_s(\mathcal{F} \otimes \mathcal{G}) \leq Sw_s(\mathcal{F})r(\mathcal{G}) + Sw_s(\mathcal{G})r(\mathcal{F}). \tag{1}$$

Grâce aux inégalités $r_s(\mathcal{F} \otimes \mathcal{G}) \geq r_s(\mathcal{F})r_s(\mathcal{G})$ et $(r(\mathcal{F}) - r_s(\mathcal{F}))(r(\mathcal{G}) - r_s(\mathcal{G})) \geq 0$, on en déduit l'inégalité :

$$r(\mathcal{F} \otimes \mathcal{G}) - r_s(\mathcal{F} \otimes \mathcal{G}) \leq (r(\mathcal{F}) - r_s(\mathcal{F}))r(\mathcal{G}) + r(\mathcal{F})(r(\mathcal{G}) - r_s(\mathcal{G})). \tag{2}$$

En additionnant les inégalités (1) et (2), on obtient l'inégalité suivante, qui nous servira pour la suite :

$$a_s(\mathcal{F} \otimes \mathcal{G}) \leq a_s(\mathcal{F})r(\mathcal{G}) + r(\mathcal{F})a_s(\mathcal{G}).$$

On fixe un plongement $\iota : \overline{\mathbb{Q}_\ell} \hookrightarrow \mathbb{C}$, et on suppose que $\mathcal{F}$ et $\mathcal{G}$ sont géométriquement irréductibles, de rang r sur U, ι-purs de même poids, non isomorphes en tant que $\overline{\mathbb{Q}_\ell}$-faisceaux sur $X_{\overline{\mathbb{F}_q}}$, et qu'ils ont même traces de Frobenius sur $U(\mathbb{F}_{q^n})$ pour un certain entier n. Notre but est de trouver une condition sur n telle que cela implique une contradiction.

On a les propriétés suivantes :

$$\begin{cases} \mathrm{H}^0(X_{\overline{\mathbb{F}_q}}, j_*(\mathcal{F}^\vee \otimes \mathcal{G})) & = & 0 \\ \mathrm{H}^2(X_{\overline{\mathbb{F}_q}}, j_*(\mathcal{F}^\vee \otimes \mathcal{G})) & = & 0 \\ \mathrm{H}^0(X_{\overline{\mathbb{F}_q}}, j_*(\mathcal{F}^\vee \otimes \mathcal{F})) & = & \overline{\mathbb{Q}_\ell} \text{ avec } \mathrm{Frob}_q \text{ agissant par multiplication par } 1 \\ \mathrm{H}^2(X_{\overline{\mathbb{F}_q}}, j_*(\mathcal{F}^\vee \otimes \mathcal{F})) & = & \overline{\mathbb{Q}_\ell} \text{ avec } \mathrm{Frob}_q \text{ agissant par multiplication par } q \end{cases}$$

Par hypothèse, on a l'égalité :

$$\sum_{x \in U(\mathbb{F}_{q^n})} \overline{\mathrm{Tr}(\mathrm{Frob}_x, \mathcal{F}_{\overline{x}})}\mathrm{Tr}(\mathrm{Frob}_x, \mathcal{G}_{\overline{x}}) = \sum_{x \in U(\mathbb{F}_{q^n})} \overline{\mathrm{Tr}(\mathrm{Frob}_x, \mathcal{F}_{\overline{x}})}\mathrm{Tr}(\mathrm{Frob}_x, \mathcal{F}_{\overline{x}}).$$

Pour alléger les notations, on omettra dans la suite les $\overline{x}$ qui indiquent les fibres sur lesquelles on exprime les traces des Frobenius.

On a l'égalité :

$$\sum_{x \in X(\mathbb{F}_{q^n})} \mathrm{Tr}(\mathrm{Frob}_x, j_*(\mathcal{F}^\vee \otimes \mathcal{G})) = \sum_{i=0}^{2} (-1)^i \mathrm{Tr}(\mathrm{Frob}_q^n, \mathrm{H}^i(X_{\overline{\mathbb{F}_q}}, j_*(\mathcal{F}^\vee \otimes \mathcal{G}))$$

(et de même pour $\mathcal{F}^\vee \otimes \mathcal{F}$). L'égalité précédente peut donc se réécrire :

$$\begin{aligned} q^n + 1 - \mathrm{Tr}(\mathrm{Frob_q^n}, \mathrm{H}^1(X_{\overline{\mathbb{F}_q}}, j_*(\mathcal{F}^\vee \otimes \mathcal{F})) + \mathrm{Tr}(\mathrm{Frob}_q^n, \mathrm{H}^1(X_{\overline{\mathbb{F}_q}}, j_*(\mathcal{F}^\vee \otimes \mathcal{G})) \\ = \sum_{x \in X(\mathbb{F}_{q^n}) \setminus U(\mathbb{F}_{q^n})} \mathrm{Tr}(\mathrm{Frob}_x, j_*(\mathcal{F}^\vee \otimes \mathcal{F})) - \mathrm{Tr}(\mathrm{Frob}_x, j_*(\mathcal{F}^\vee \otimes \mathcal{G})) \end{aligned}.$$

Comme les faisceaux $\mathcal{F}^\vee \otimes \mathcal{G}$ et $\mathcal{F}^\vee \otimes \mathcal{F}$ sont purs de poids 0, on a par [5, Lemme 1.8.1] l'inégalité :

$$\left| \sum_{x\in X(\mathbb{F}_{q^n})\setminus U(\mathbb{F}_{q^n})} \mathrm{Tr}(\mathrm{Frob}_x, j_*(\mathcal{F}^\vee \otimes \mathcal{F})) - \mathrm{Tr}(\mathrm{Frob}_x, j_*(\mathcal{F}^\vee \otimes \mathcal{G}))\right| \\ \leq \sum_{s\in S,\ \deg s \ \mid\ n} \deg s \left(r_s(\mathcal{F}^\vee \otimes \mathcal{G}) + r_s(\mathcal{F}^\vee \otimes \mathcal{F})\right).$$

De plus, comme les H^1 qui apparaissent ci-dessus sont purs de poids 1 :

$$\begin{array}{rcl} \left|\mathrm{Tr}(\mathrm{Frob}_q^n, \mathrm{H}^1(X_{\overline{\mathbb{F}_q}}, j_*(\mathcal{F}^\vee \otimes \mathcal{F}))\right| & \leq & q^{\frac{n}{2}} \dim\left(\mathrm{H}^1(X_{\overline{\mathbb{F}_q}}, j_*(\mathcal{F}^\vee \otimes \mathcal{F}))\right) \\ & = & q^{\frac{n}{2}}\left(r^2(2g-2) + \sum_{s\in S} a_s(\mathcal{F}^\vee \otimes \mathcal{F}) + 2\right) \\ \left|\mathrm{Tr}(\mathrm{Frob}_q^n, \mathrm{H}^1(X_{\overline{\mathbb{F}_q}}, j_*(\mathcal{F}^\vee \otimes \mathcal{G}))\right| & \leq & q^{\frac{n}{2}} \dim\left(\mathrm{H}^1(X_{\overline{\mathbb{F}_q}}, j_*(\mathcal{F}^\vee \otimes \mathcal{G}))\right) \\ & = & q^{\frac{n}{2}}\left(r^2(2g-2) + \sum_{s\in S} a_s(\mathcal{F}^\vee \otimes \mathcal{G})\right) \end{array}$$

On a aussi les inégalités :

$$\begin{array}{rcl} a_s(\mathcal{F}^\vee \otimes \mathcal{F}) & \leq & 2r\, a_s(\mathcal{F}) \\ a_s(\mathcal{F}^\vee \otimes \mathcal{G}) & \leq & r(a_s(\mathcal{F}) + a_s(\mathcal{G})) \end{array}.$$

En majorant bêtement $r_s(\mathcal{F}^\vee \otimes \mathcal{G})$ et $r_s(\mathcal{F}^\vee \otimes \mathcal{F})$ par r^2, on en déduit qu'on a une contradiction dès que :

$$q^n \geq q^{\frac{n}{2}}\left(2r^2(2g-2) + r(\sum_{s\in S} 3a_s(\mathcal{F}) + a_s(\mathcal{G})) + 2\right) + 2r^2\left(\sum_{s\in S,\ \deg s\ \mid\ n} \deg s\right). \tag{3}$$

On déduit finalement le théorème suivant, variante du résultat de Deligne [6, Lemme 2.6] :

Théorème 2.1. *Soient $\mathcal{F}, \mathcal{G}$ deux $\mathbb{Q}_\ell$-faisceaux lisses sur U, géométriquement irréductibles, de rang r sur U, purs de même poids, non isomorphes en tant que $\overline{\mathbb{Q}_\ell}$-faisceaux sur $X_{\overline{\mathbb{F}}_q}$, et qui ont mêmes traces de Frobenius sur $U(\mathbb{F}_{q^n})$. Alors n vérifie l'inégalité* (3).

2.3. **Lien avec les formes automorphes.** Supposons que $\mathcal{F}$ correspond à une forme automorphe cuspidale π pour GL_r. Alors π est générique, et d'après [11] π_v est non ramifiée en dehors de S.

On pose pour $v \in S$:

$$a_v(\pi_v) = \min\left\{ m \text{ tel que } \pi_v \text{ a un vecteur invariant non nul par } K_r(m)\right\},$$

où :

$$\begin{cases} K_r(m) = \left\{\begin{pmatrix} h & z \\ y & x\end{pmatrix} \in \mathrm{GL}_r(\mathcal{O}_v),\ h \in \mathcal{M}_{r-1}(\mathcal{O}_v),\ x \equiv 1 \bmod \varpi_v^m,\ y \equiv 0 \bmod \varpi_v^m\right\}\ ; \\ \mathcal{O}_v \text{ est l'anneau des entiers de } \mathcal{F}_v\ ; \\ \varpi_v \text{ est une uniformisante.} \end{cases}$$

On appelle $a_v(\pi_v)$ le conducteur de π_v. D'après [11] et [13], on a l'égalité : $a_v(\pi_v) = a_v(\mathcal{F})$.

Soient π, π' sont deux formes automorphes cuspidales pour GL_r, non ramifiées sur $U = X \setminus S$, et non induites de formes automorphes sur $X_{\mathbb{F}_{q^m}}$ pour $\mathrm{GL}_{r/m}$ avec $m > 1$. Cette dernière condition se voit facilement sur les valeurs propres de Hecke, qui doivent, pour tout premier m divisant r, être non toutes nulles pour les places de degré non multiple de m.

Le résultat suivant transcrit dans le cadre des formes automorphes la variante de [6, Lemme 2.6] expliquée en détail au paragraphe précédent.

Théorème 2.2. *On considère π, π' comme ci-dessus. On note* St *la représentation standard de* GL_r*, et on suppose que les valeurs propres de Hecke de π et π' en les place $v \in U$ de degré $\deg v | n$ pour les représentations* $\Lambda^i \mathrm{St}$ *($i \leq n/\deg v$) coïncident pour un entier n vérifiant :*

$$q^n \geq q^{\frac{n}{2}} \left(2r^2(2g-2) + r(\sum_{v \in S} 3a_v(\pi_v) + a_v(\pi'_v)) + 2 \right) + 2r^2 \left(\sum_{v \in S,\ \deg v \ | \ n} \deg v \right).$$

Alors π et π' sont isomorphes, à torsion près par un caractère dont la puissance n-ème est triviale.

On verra dans le paragraphe 4.1 dans quelle mesure cette condition est optimale (en la comparant à une minoration de la dimension d'espaces de formes automorphes suivant [7]).

3. Le cas des corps de nombres

3.1. **Rappels et notations.** Considérons un $\mathbb{Q}$-groupe semi-simple G, forme intérieure d'un groupe déployé, et son algèbre de Lie $\mathfrak{g}$. On note $\widehat{G}$ le dual de Langlands de G (qui est un $\mathbb{C}$-groupe semi-simple dont la donnée radicielle est duale à celle de G), et $\widehat{\mathfrak{g}}$ son algèbre de Lie.

On considère une représentation automorphe cuspidale π de $G(\mathbb{A})$. On associe à π :

– une classe de conjugaison semi-simple $c_\infty(\pi)$ dans $\widehat{\mathfrak{g}}$, appelée "caractère infinitésimal" de π (suivant l'isomorphisme d'Harish-Chandra) ;
– pour tout nombre premier p non ramifié, une classe de conjugaison semi-simple $c_p(\pi)$ dans $\widehat{G}$, appelée "paramètre de Satake en p" de π (suivant l'isomorphisme de Satake).

Donnons-nous $r : \widehat{G} \to \mathrm{GL}_d$ une représentation injective. Par abus de notation, on notera aussi $r : \widehat{\mathfrak{g}} \to \mathrm{M}_d$ la représentation induite par r sur $\widehat{\mathfrak{g}}$ (où M_d désigne l'algèbre des matrices carrées de tailles d, qui n'est autre que l'algèbre de Lie de GL_d).

Suivant ces notations, la donnée de $r(c_p(\pi))$ est équivalente à la donnée de complexes tous non nuls $\alpha_i(p)$ ($i \in \{1, \ldots, d\}$) (qui sont les valeurs propres de $r(c_p(\pi))$). Les $\alpha_i(p)$ sont les "racines locales en p" de la fonction L associée à π et r.

En les p pour lesquels π est ramifiée, on possède aussi des nombres complexes $\alpha_i(p), i \in \{1, \ldots, d\}$, dont l'un au moins est nul, tels que le facteur L local soit $\prod_{j=1}^d \left(1 - p^{-s}\alpha_i(p)\right)^{-1}$, et qu'on appelle aussi "racines locales en p".

La fonction L associée à π dépend du choix d'une représentation $r : \widehat{G} \to \mathrm{GL}_d$. En pratique, lorsque $\widehat{G}$ est un groupe classique, on prendra pour r la représentation standard de $\widehat{G}$, et on omettra parfois r dans les arguments de la fonction L.

La fonction L associée à π et r est définie par :

$$\begin{aligned} L(\pi, r, s) &= \left(\prod_{\substack{p \text{ premier} \\ p \text{ ramifié}}} \prod_{j=1}^d \left(1 - p^{-s}\alpha_i(p)\right)^{-1} \right) \left(\prod_{\substack{p \text{ premier} \\ p \text{ non ramifié}}} \det\left(1 - p^{-s} r(c_p(\pi))\right)^{-1} \right). \\ &= \prod_{p \text{ premier}} \prod_{j=1}^d \left(1 - p^{-s}\alpha_i(p)\right)^{-1} \end{aligned}$$

Le "degré" de $L(\pi, r, s)$ est la dimension de la représentation $r : \widehat{G} \to \mathrm{GL}_d$.

Les "composantes locales en l'infini" de $L(\pi, r, s)$ sont les valeurs propres de $r(c_\infty(\pi))$. La donnée des composantes locales en l'infini est donc imposée par la donnée du caractère infinitésimal et de la représentation r.

Le "facteur gamma" à l'infini de $L(\pi, r, s)$ est une fonction qui ne dépend que des valeurs propres de $r(c_\infty(\pi))$. Deux représentations automorphes π, π' ont des fonctions L

avec les mêmes facteurs gamma si elles ont même caractère infinitésimal. Si l'on note $\kappa_j, j \in \{1, \dots, d\}$ les composantes locales en l'infini de $L(\pi, r, s)$, le facteur gamma à l'infini de $L(\pi, r, s)$ est donné par :

$$\gamma(\pi, r, s) = \pi^{-ds/2} \prod_{j=1}^{d} \Gamma\left(\frac{s+\kappa_j}{2}\right).$$

Les "racines locales en p" de $L(\pi, r, s)$ sont les $\alpha_i(p)$. Lorsque π est non ramifiée en p, ce sont donc les valeurs propres du paramètre de Satake en p de π. En particulier, deux représentations automorphes π, π' qui sont non ramifiées en p ont mêmes racines locales en p si elles ont même paramètre de Satake en p.

Le "conducteur" de $L(\pi, r, s)$ est un entier $q(\pi)$ qui vérifie que toutes les racines locales en un nombre premier p sont toutes non nulles si, et seulement si, p ne divise pas $q(\pi)$. En particulier, π est ramifiée en p si, et seulement, p divise $q(\pi)$.

Le "conducteur analytique" de $L(\pi, r, s)$, noté $\mathfrak{q}(\pi)$, s'exprime en fonction de $q(\pi)$ et des composantes locales en l'infini κ_j de π de la manière suivante : $\mathfrak{q}(\pi) = q(\pi) \cdot \prod_{j=1}^{d} (|\kappa_j| + 3)$.

En pratique, les seules fonctions L que l'on considérera seront celles associées à des représentations tempérées. En particulier, une représentation π tempérée vérifie que :

– les racines locales en les places non ramifiées sont toutes de module 1 ;

– les racines locales en les places ramifiées sont soit nulles, soit de module 1.

On se limitera dans la suite aux fonctions L associées aux représentations automorphes tempérées des groupes linéaires. On allégera alors les notations, en prenant pour r la représentation "identité", et on l'ometttra dans les arguments des fonctions L considérées.

Dans ce cas, deux fonctions $L(\pi, s)$ et $L(\pi', s)$ ont même facteurs gamma (respectivement mêmes racines locales en p) si, et seulement si, les représentations π et π' ont même caractère infinitésimal (respectivement même paramètre de Satake en p). Dans le cas général, comme évoqué ci-dessus, on n'avait qu'une seule implication.

La théorie développée par Arthur [1], complétée par les travaux récents de Waldspurger notamment [15] [17] (qu'il serait trop long de développer en détail ici), ramène l'étude des représentations automorphes des groupes classiques à celles des groupes linéaires, et rend ce choix légitime.

Pour faire court, disons simplement que les paramètres de Satake de représentations tempérées s'expriment comme "sommes directes" des paramètres de Satake de représentations automorphes tempérées des groupes linéaires. En termes de fonctions L, cela se traduit par le fait que les fonctions L associées à des représentations tempérées des groupes classiques s'écrivent comme produits des fonctions L associées à des représentations tempérées des groupes linéaires.

Finissons par quelques explications sur les fonctions L de Rankin–Selberg, suivant [10, §5.1] par exemple. Soient π et π' des représentations automorphes tempérées de PGL_d et PGL_e respectivement. On considère $L(\pi, s)$ et $L(\pi', s)$ les fonctions L qui leur sont associées, de composantes locales en l'infini respectivement les κ_i et les ν_i, et de racines locales respectivement les $\alpha_i(p)$ et les $\beta_i(p)$. On dit que l'on a une convolution de Rankin–Selberg s'il existe une fonction L, notée $L(\pi \otimes \pi', s)$, de degré $d \cdot e$ telle que :

– on a une égalité de la forme :

$$L(\pi \otimes \pi', s) = \left(\prod_{p \nmid q(\pi)q(\pi')} L_p(s)\right) \left(\prod_{p \mid q(\pi)q(\pi')} H_p(s)\right)$$

où les fonctions L_p sont définies par :

$$L_p(s) = \prod_{i,j} (1 - \alpha_i(p)\beta_j(p)p^{-s})^{-1}$$

et fonctions H_p sont définies par :

$$H_p(s) = \prod_{i=1}^{de}(1 - \gamma_i(p)p^{-s})^{-1}$$

pour des complexe $\gamma_i(p)$ de module au plus p (et seront même des complexes de module 0 ou 1) ;

– le facteur gamma en l'infini de $L(\pi \otimes \pi', s)$ s'écrit :

$$\gamma(\pi \otimes \pi', s) = \pi^{-des/2} \prod_{i,j} \Gamma\left(\frac{s + \mu_{i,j}}{2}\right)$$

où les $\mu_{i,j}$ sont des complexes tels que $\mathrm{Re}(\mu_{i,j}) \leq \mathrm{Re}(\kappa_i + \nu_j)$ et $|\mu_{i,j}| \leq |\kappa_i| + |\nu_j|$;

– le conducteur de $L(\pi \otimes \pi', s)$ est un diviseur de $q(\pi)^e q(\pi')^d$.

Suivant les résultats de Jacquet–Shalika ([12, I] si $d = e$ et [12, II] si $d \neq e$), la convolution de Rankin–Selberg existe bien pour π, π' des représentations automorphes tempérées de PGL_d et PGL_e.

3.2. **Le résultat d'Iwaniec–Kowalski.** Le théorème suivant est alors une conséquence immédiate du résultat d'Iwaniec–Kowalski [10, Proposition 5.22].

Théorème 3.1. *Soient π, π' deux représentations automorphes tempérées de* PGL_d *non isomorphes. On suppose que GRH est vérifiée pour les deux fonctions de Rankin–Selberg $L(\pi \otimes \overline{\pi}, s)$ et $L(\pi \otimes \overline{\pi'}, s)$.*

Alors il existe un nombre premier $p \leq C\left(d \log \mathfrak{q}(\pi)\mathfrak{q}(\pi')\right)^2$, non ramifié pour π et π', tel que $c_p(\pi) \neq c_p(\pi')$, pour C une constante universelle positive.

Démonstration. Il suffit juste d'appliquer [10, Proposition 5.22]. On se contente d'expliquer les différences entre notre théorème et le résultat d'Iwaniec–Kowalski.

L'énoncé de [10] demandait uniquement que les racines locales en les places ramifiées soient de module ≤ 1. On a remplacé cette condition par le fait que les représentations π et π' sont tempérées (qui est une condition en toutes les places). La raison est que, suivant la définition des fonctions L adoptées par [10], les racines locales en les places p non ramifiées doivent être de module 1. Le fait de considérer uniquement des représentations tempérées est une condition plus forte, mais qui permet d'avoir les conditions sur les racines locales en les places ramifiées et non ramifiées simultanément.

Ensuite, on a omis la condition sur l'existence des fonctions de Rankin–Selberg $L(\pi \otimes \overline{\pi}, s)$ et $L(\pi \otimes \overline{\pi'}, s)$. Suivant les résultats de Jacquet–Shalika [12], ces fonctions L sont bien définies dans la mesure où on a supposé que π, π' étaient des représentations automorphes tempérées de PGL_d.

Enfin, on a remplacé la condition que la fonction $L(\pi \otimes \overline{\pi'}, s)$ est entière par le fait que les représentations π et π' sont non isomorphes. Cette seconde condition est plus faible, puisque la fonction $L(\pi \otimes \overline{\pi'}, s)$ est entière si, et seulement si, les représentations π et π' n'admettent pas de facteurs isomorphes.

Supposons que π et π' ne sont pas isomorphes, mais que $L(\pi \otimes \overline{\pi'}, s)$ n'est pas entière. Alors on peut considérer π_0 le facteur commun à π et π' le plus grand (en termes de rang), et on écrit : $\pi = \pi_0 \oplus \pi_1$ et $\pi' = \pi_0 \oplus \pi'_1$. En termes de fonctions L, cela se traduit par les égalités :

$$L(\pi, s) = L(\pi_0, s) \cdot L(\pi_1, s) \quad \text{et} \quad L(\pi', s) = L(\pi_0, s) \cdot L(\pi'_1, s)$$

En divisant par $L(\pi_0, s)$, on se ramène à l'étude des fonctions $L(\pi_1, s)$ et $L(\pi'_1, s)$, auxquelles on voudrait appliquer [10, Proposition 5.22]. Il suffit en fait de constater que les fonctions $L(\pi_1 \otimes \overline{\pi_1}, s)$ et $L(\pi_1 \otimes \overline{\pi'_1}, s)$ sont obtenues en divisant les fonctions $L(\pi \otimes \overline{\pi}, s)$ et $L(\pi \otimes \overline{\pi'}, s)$

par les produit de fonctions L de Rankin–Selberg $L(\pi_0\otimes\overline{\pi_0},s)\cdot L(\pi_0\otimes\overline{\pi_1},s)\cdot L(\pi_1\otimes\overline{\pi_0},s)$ et $L(\pi_0\otimes\overline{\pi_0},s)\cdot L(\pi_0\otimes\overline{\pi_1'},s)\cdot L(\pi_1'\otimes\overline{\pi_0},s)$:

– les fonctions $L(\pi_1,s)$ et $L(\pi_1',s)$ ont évidemment même degré, comme les fonctions $L(\pi,s)$ et $L(\pi',s)$ ont même degré et qu'on les a divisées par la même fonction $L(\pi_0,s)$;
– pour les mêmes raisons, les fonctions $L(\pi_1,s)$ et $L(\pi_1',s)$ ont aussi même facteur gamma en l'infini ;
– les fonctions $L(\pi_1\otimes\overline{\pi_1},s)$ et $L(\pi_1\otimes\overline{\pi_1'},s)$ existent bien ;
– la fonction $L(\pi_1\otimes\overline{\pi_1'},s)$ est entière, par maximalité de la dimension de π_0 ;
– les racines locales en les places ramifiées de $L(\pi_1\otimes\overline{\pi_1},s)$ et $L(\pi_1\otimes\overline{\pi_1'},s)$ sont incluses dans les racines locales en les places ramifiées de $L(\pi\otimes\overline{\pi},s)$ et $L(\pi\otimes\overline{\pi'},s)$, et sont donc de modules ≤ 1 ;
– les zéros des fonctions $L(\pi_1\otimes\overline{\pi_1},s)$ et $L(\pi_1\otimes\overline{\pi_1'},s)$ sont aussi des zéros des fonctions $L(\pi\otimes\overline{\pi},s)$ et $L(\pi\otimes\overline{\pi'},s)$, donc les fonctions $L(\pi_1\otimes\overline{\pi_1},s)$ et $L(\pi_1\otimes\overline{\pi_1'},s)$ vérifient bien GRH.

On peut donc appliquer [10, Proposition 5.22] aux fonctions $L(\pi_1\otimes\overline{\pi_1},s)$ et $L(\pi_1\otimes\overline{\pi_1'},s)$.

En notant d_1 le degré de ces fonctions L, il existe $p\leq C\left(d_1\log\mathfrak{q}(\pi_1)\mathfrak{q}(\pi_1')\right)^2$ non ramifié pour π_1 et π_1' (et donc non ramifié pour π et π') tel que $c_p(\pi_1)\neq c_p(\pi_1')$ (et donc $c_p(\pi)\neq c_p(\pi')$).

Il suffit ensuite de constater que $d_1\leq d$, $\mathfrak{q}(\pi_1)\leq\mathfrak{q}(\pi)$ et $\mathfrak{q}(\pi_1')\leq\mathfrak{q}(\pi')$ pour conclure que le nombre premier p en question vérifie l'inégalité : $p\leq C\left(d\log\mathfrak{q}(\pi)\mathfrak{q}(\pi')\right)^2$. □

3.3. **Quelques remarques.** On peut déjà comparer les deux résultats que l'on a, sur les corps de fonctions et sur les corps de nombres.

On peut voir que, dans le cas des corps de nombres, on avait les hypothèses équivalentes suivantes :

– $\mathcal{F}$ et $\mathcal{G}$ géométriquement irréductibles (lorsque l'on raisonne sur des faisceaux) ;
– π et π' non induites de $\mathbb{F}_{q^m}$, avec $m>1$ (lorsque l'on raisonne sur des formes automorphes).

Il n'est pas surprenant qu'une hypothèse analogue n'apparaisse pas dans le cas des corps de nombres, puisqu'il n'existe pas d'analogue à ces hypothèses pour les corps de nombres.

Toujours pour comparer le cas des corps de nombres à celui des corps de fonctions, notons que l'inégalité $\mathfrak{q}(\pi\otimes\pi')\leq(\mathfrak{q}(\pi)\mathfrak{q}(\pi'))^d$ (utilisée pour la démonstration de [10, Proposition 5.22]) est l'analogue de l'inégalité $\sum_{s\in S}a_s(\mathcal{F}\otimes\mathcal{G})\leq\sum_{s\in S}r(a_s(\mathcal{F})+a_s(\mathcal{G}))$ (utilisée pour la démonstration de [6, Lemme 2.6]).

En effet, dans le cas des corps de nombres, si l'on suppose que le faisceau $\mathcal{F}$ de rang r correspond à une forme automorphe cuspidale π pour GL_r, alors le conducteur de π est donné par : $\mathfrak{q}(\pi)=q^{r(2g-2)+\sum_s a_s(\mathcal{F})}$. Les deux inégalités $\mathfrak{q}(\pi\otimes\pi')\leq(\mathfrak{q}(\pi)\mathfrak{q}(\pi'))^d$ et $\sum_{s\in S}a_s(\mathcal{F}\otimes\mathcal{G})\leq\sum_{s\in S}r(a_s(\mathcal{F})+a_s(\mathcal{G}))$ sont alors bien analogues, puisque dans le cas des corps de nombres on s'était placé sur $\mathbb{Q}$, ce qui implique que l'analogue de $2g-2$ est 0 (suivant la formule de Poisson, analogue de Riemann–Roch).

Finissons par quelques explications supplémentaires concernant la constante C qui apparaît dans [10, Proposition 5.22], et dans le théorème 3.1. Une constante C qui convient a été calculée explicitement par Euvrad dans [9, Théorème 1.5]. Dans la suite, on prendra pour C la valeur explicite donnée dans [9], et on la notera C_{Euv} pour éviter toute ambiguïté.

4. Étude de l'optimalité des résultats exposés

4.1. **Le cas des corps de fonctions.** Notre but ici est de voir à quel point le résultat du théorème 2.2 est optimal. Pour cela, on veut estimer le nombre de formes automorphes dans un cas particulier, puis en déduire une borne optimale théorique sur le nombre minimal d'opérateurs de Hecke à calculer pour distinguer deux formes automorphes, et enfin de comparer ce résultat aux bornes données par le théorème 2.2. Le comptage que l'on fait repose sur les résultats de Deligne–Flicker [7] que l'on expose ci-dessous.

Soit X une courbe projective lisse géométriquement irréductible sur $\mathbb{F}_q$, et S un ensemble fini de places de X, que l'on suppose non vide. Alors on a une bijection entre :

– les classes d'isomorphismes à $\mathbb{F}_q$-torsion près de $\overline{\mathbb{Q}_\ell}$-faisceaux lisses de rang r sur $X \setminus S$, dont la monodromie en les places de S est modérée et telle que le groupe d'inertie agit par un unipotent régulier ;

– les classes d'isomorphismes à $\mathbb{F}_q$-torsion près de représentations automorphes cuspidales pour GL_r, dont le facteur en les places $v \in S$ est de la forme Steinberg $\otimes\, \chi(\det)$.

On note $T(X, S, r)$ le cardinal de ces deux ensembles, qui est calculé par Deligne–Flicker [7, Theorem 2.3]. Afin de simplifier les formules, on suppose que r est premier, et ne divise aucun $\deg s$ pour $s \in S$. On note de plus :

$$f(t) = \prod_{i=1}^{2g}(1-\alpha_i t) = \det\left(1 - t\mathrm{Frob}_q, \mathrm{H}^1(X_{\overline{\mathbb{F}_q}}, \overline{\mathbb{Q}_\ell})\right)$$

où les $\alpha_i,\ i \in \{1, \dots, 2g\}$ sont algébriques et ont une norme $\sqrt{q}$ en toutes les places archimédiennes (d'après [5]).

On a alors :

$$\begin{aligned} T(X,S,r) =& (q-1)f(1)\frac{1}{q^r-1}\prod_{j=1}^{r-1}\left\{\frac{1}{(q^j-1)^2}f(q^j)\prod_{s\in S}(1-q^{j\deg s})\right\} \\ & + c_r r^{N_1-2}\prod(1-\alpha_i^r)\frac{1}{q^r-1} \; - (-1)^{N_1(r-1)}f(1) \end{aligned}$$

où :

– $c_r = \sharp\{x \in \mathbb{F}_{q^r}^* \ ,\ x \text{ engendre } \mathbb{F}_{q^r} \text{ sur } \mathbb{F}_q\} = q^r - q$;

– $N = \sum_{s\in S} \deg s$;

– $N_1 = \sum_{s \in S} 1 = |S|$.

On suppose que $\left(1 - \frac{1}{\sqrt{q}}\right)^g \geq 1/2$, et on rappelle que $\prod \alpha_i = q^g$. On suppose que q, N, g sont fixés, et ne sont pas trop petits (c'est-à-dire qu'ils sont plus grands qu'une constante universelle M). Alors $T(X, S, r)$ est équivalent pour r grand, à une constante multiplicative non nulle près, à :

$$\begin{aligned} & q \cdot q^g \cdot \frac{1}{q^r} \cdot \prod_{j=1}^{r-1}\left\{q^{-2j}q^{g(2j+1)}\prod_{s\in S}q^{j\deg s}\right\} \\ & = q^{g+1-r-r(r-1)+g(r^2-1)+N\frac{r(r-1)}{2}} \end{aligned}$$

En effet, suivant l'écriture précédente de $T(X, S, r)$, les deuxième et troisième termes sont respectivement en $q^{rg} \cdot r^{N_1-2}$ et q^g. Ils sont donc bien négligeables devant la quantité précédente.

Notons enfin que, toujours pour $q, N, g \geq M$ fixés, et r grand, le terme dominant dans l'exposant est $\left(g - 1 + \frac{N}{2}\right) r^2$. C'est ce terme qui nous intéressera dans la suite, puisque c'est la quantité $\log\left(T(X, S, r)\right)$ qui sera pertinente pour nous.

Supposons que, pour un entier n, les classes à $\mathbb{F}_q$-torsion près de formes automorphes comme ci-dessus soient déterminées par leurs traces de Frobenius sur $(X \setminus S)(\mathbb{F}_{q^n})$. Et supposons de plus que n est premier (pour simplifier).

En termes d'information, ces traces contiennent chacune au plus (nr) q-bit (où on entend par q-bit la donnée d'un élément de $\mathbb{F}_q$). Comme il y a $\frac{q^n-q}{n}$ places (puisque n est premier), cela représente en tout $r(q^n-q) \sim rq^n$ q-bits.

Ces traces de Frobenius ne peuvent pas contenir moins d'information que la connaissance des classes de formes automorphes à $\mathbb{F}_q$ torsion près. Pour q, N, g fixés et r grand, le logarithme en base q de ce nombre de classes est équivalent à $\left(g-1+\frac{N}{2}\right)r^2$, et donc qu'elles représentent à une constante multiplicative près $\left(g-1+\frac{N}{2}\right)r^2$ q-bits en termes d'information.

On en déduit que l'on a nécessairement une inégalité de la forme : $rq^n \geq \left(g-1+\frac{N}{2}\right)r^2$ (à une constante multiplicative près), et donc finalement, toujours à une constante multiplicative près :

$$q^n \geq \left(g-1+\frac{N}{2}\right)r\cdot$$

Revenons maintenant au résultat du théorème 2.2. Suivant ce résultat, il est suffisant que

$$q^n \geq \left((4g-4+4N)\,r^2\right)^2$$

pour que les traces des Frobenius sur $(X \setminus S)(\mathbb{F}_{q^n})$ déterminent la classe à $\mathbb{F}_q$-torsion d'une forme automorphe.

On peut quantifier l'écart entre la borne donnée par le théorème 2.2 et la borne optimale théorique précédente de la façon suivante. Fixons q, g, N, en les supposant suffisamment grands, et faisons tendre r vers l'infini. À des constantes multiplicatives près (qui dépendent de q, g et N), on a la situation suivante : r^5 q-bits sont suffisants pour distinguer des formes automorphes par leurs petites valeurs propres de Hecke, tandis que r^2 q-bits sont nécessaires.

4.2. **Le cas des corps de nombres.** On se restreint ici aux cas des représentations automorphes cuspidales algébriques tempérées de PGL_d, éventuellement ramifiées en certaines places. Le fait qu'elles soient tempérées est nécessaire pour leur appliquer le théorème 3.1 (toujours en supposant que les hypothèses de GRH sont vérifiées pour certaines fonctions L).

Le problème est que, en général, il est impossible de compter toutes les représentations automorphes comme ci-dessus, à caractère infinitésimal fixé (ou, en termes de fonctions L, à facteur gamma fixé).

Dans le cas où les représentations considérées sont supposées de plus autoduales et non ramifiées en toutes les places, seul les cas $d=2$ et $d=3$sont bien connus, auxquels cas ces représentations proviennent des formes modulaires classiques pour $\mathrm{SL}_2(\mathbb{Z})$. Pour $d=4$ ou $d=5$, elles peuvent être construites à l'aide de formes modulaires classiques pour $\mathrm{SL}_2(\mathbb{Z})$ et de formes modulaires de Siegel de genre 2 pour $\mathrm{Sp}_4(\mathbb{Z})$. Pour d plus grand, il s'agit du problème étudié par Chenevier–Renard [2] pour les cas des groupes PGL_6, PGL_7 et PGL_8. Mais leurs résultats ne donnent en aucun cas de formule générale. On renvoie d'ailleurs à [2] pour davantage d'informations sur les cas $d \leq 5$.

Dans notre cas plus général (c'est-à-dire avec de la ramification, et des représentations non nécessairement autoduales), la situation est beaucoup plus compliquée. Le seul cas que l'on sait bien décrire est $d=2$. Auquel cas, la représentation considérée provient d'une forme modulaire de niveau N, suivant la construction développée ci-dessous. Dès lors que $d \geq 3$, même en supposant qu'il n'y a pas ramification, on n'est pas en mesure de compter les représentations de PGL_d qui nous intéressent.

On va donc se restreindre ici au cas où $d=2$, et on va appliquer le théorème 3.1. Dans ce cas, on peut construire des représentations automorphes à partir de formes modulaires paraboliques pour le groupe

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}),\ a \equiv d \equiv 1 \bmod N,\ c \equiv 0 \bmod N \right\}.$$

On s'intéressera à l'espace des formes parabolique de poids k pour $\Gamma_1(N)$, dont on notera $s_k(N)$ la dimension. En pratique, on fera tendre N et k vers l'infini, et on peut donc supposer que $N, k \geq 3$, auquel cas on a l'égalité suivante :

$$s_k(N) = \frac{k-1}{12} d_N - \frac{d_N}{2N}, \tag{4}$$

où $d_N = \frac{1}{2} N^3 \prod_{p|N} (1 - p^{-2})$ est, à un facteur 1/2 près, l'indice du sous-groupe principal de niveau N dans $\mathrm{SL}_2(\mathbb{Z})$.

Pour avoir des notations qui correspondent davantage à celles de Deligne [4], on préférera utiliser le groupe

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}),\ c \equiv 0 \bmod N \right\}$$

et voir nos formes modulaires pour $\Gamma_0(N)$ comme des formes modulaires pour $\Gamma_0(N)$ munies d'un caractère $\varepsilon : (\mathbb{Z}/N\mathbb{Z})^* \to \mathbb{C}^*$, c'est-à-dire telles que :

$$\forall \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N), f\left(\frac{az+b}{cz+d}\right) = \varepsilon(a)^{-1}(cz+d)f(z).$$

Pour alléger les notations, on notera aussi $\varepsilon : \mathbb{Z}/N\mathbb{Z} \to \mathbb{C}$ le prolongement de ε à $\mathbb{Z}/N\mathbb{Z}$ en posant $\varepsilon(a) = 0$ si $\mathrm{pgcd}(a, N) \neq 1$, et aussi $\varepsilon : \mathbb{Z} \to \mathbb{C}$ son prolongement à $\mathbb{Z}$ associé à la projection naturelle $\mathbb{Z} \to \mathbb{Z}/N\mathbb{Z}$.

Donnons-nous $f = \sum a_n q^n$ une forme modulaire parabolique normalisée pour $\Gamma_1(N)$ (qu'on peut voir comme une forme modulaire pour $\Gamma_0(N)$ de caractère ε) de poids k, propre pour les opérateurs de Hecke T_p ($p \nmid N$). On lui associe une représentations automorphe cuspidale algébrique régulière π de PGL_2 qui vérifie :

- les composantes locales en l'infini sont $\pm\frac{k-1}{2}$;
- pour tout $p \nmid N$ premier, les racines locales en p sont les racines du polynôme : $X^2 - \frac{a_p}{p^{(k-1)/2}} X + \varepsilon(p) \cdot p^{k-1}$.

Suivant un résultat de Deligne [4], les racines locales en les places non ramifiées sont bien toutes de module 1.

En les $p \mid N$ premiers, on ne sait a priori rien sur les racines locales en p. Plus précisément, on ne sait même pas si la représentation π est ramifiée en p ou non.

Pour pouvoir en dire davantage, on se restreint aux cas où f est une "forme nouvelle", c'est-à-dire qu'elle n'est pas une forme modulaire pour un groupe $\Gamma_1(N/l)$, où $l > 1$ divise N. Auquel cas, la représentation π est ramifiée en p, et les racines locales en p sont les racines du polynôme : $X^2 - \frac{a_p}{p^{(k-1)/2}} X$.

Pour alléger les notations, on appellera dans la suite "forme primitive de poids k et niveau N" une forme modulaire parabolique de poids k pour le groupe $\Gamma_1(N)$, propre pour les opérateurs de Hecke, et qui est une forme nouvelle. Si l'on note $s_k^{new}(N)$ le nombre de telles formes, on a l'inégalité :

$$s_k^{new}(N) \geq \left(s_k(N) - \sum_{p|N \text{ premier}} s_k(N/p) \right). \tag{5}$$

Suivant l'expression de $s_k(N)$ de (4), on en déduit que, pour tout p premier divisant N :

$$s_k(N/p) \leq \frac{k-1}{12} d_{N/p} \leq \frac{k-1}{12} \frac{d_N}{p^3 - 1/p}. \tag{6}$$

En particulier, si l'on note $\alpha = 1 - \sum_{p \text{ premier}} \frac{1}{p^3 - 1/p} \simeq 0.8$, on déduit que :

$$\alpha \frac{k-1}{12} d_N - \frac{d_N}{2N} \leq s_k^{new}(N) \leq \frac{k-1}{12} d_N - \frac{d_N}{2N}. \tag{7}$$

Disons enfin que, étant donnée une forme primitive f de poids k et niveau N, la représentation de PGL_2 qui lui est associée a pour fonction L :

$$L(\pi, s) = \prod_{p \nmid N} \frac{1}{1 - a_p p^{-s} + \varepsilon(p) p^{k-1-2s}} \cdot \prod_{p \mid N} \frac{1}{1 - a_p p^{-s}} = \prod_{p} \frac{1}{1 - a_p p^{-s} + \varepsilon(p) p^{k-1-2s}}$$

où on rappelle que l'on fait l'abus de notation $\varepsilon : \mathbb{Z} \to \mathbb{C}$, avec $\varepsilon(p) = 0$ si $p \mid N$.

Le théorème suivant est une conséquence de 3.1. Il s'agit d'une reformulation de [9, Corollaire 1.7], exprimée en termes de représentations automorphes :

Théorème 4.1. *Soient $f = \sum a_n q^n, f' = \sum a'_n q^n$ deux formes primitives de poids au plus k, de niveau divisant N, qu'on voit comme des formes modulaires pour $\Gamma_0(N)$ de caractères respectifs ε et ε', qui engendrent des représentations automorphes π et π' de* PGL_2.

On suppose que les deux fonctions $L(\pi \otimes \overline{\pi}, s)$ et $L(\pi \otimes \overline{\pi'}, s)$ vérifient GRH. Alors il existe un nombre premier p avec

$$p \nmid N \quad \text{et} \quad p \leq 16 C_{\mathrm{Euv}} \log^2 \left(N \left(3 + \frac{k+1}{2} \right)^2 \right)$$

tel que : $a_p \neq a'_p$ ou $\varepsilon(p) \neq \varepsilon'(p)$.

Démonstration. On se contente d'expliquer les différences avec le résultat initial de Euvrard [9].

La première différence concerne le niveau des formes modulaires considérées. On raisonne ici en prenant N un multiple commun des poids de f et f'.

L'autre différence est la conclusion de [9, Corollaire 1.7] : on a remplacé que "les paramètres locaux en p sont différents" par "$a_p \neq a'_p$ ou $\varepsilon(p) \neq \varepsilon'(p)$". Comme le nombre p considéré est non ramifié, alors les racines locales en p de π (respectivement de π') sont les racines du polynôme $X^2 - \frac{a_p}{p^{(k-1)/2}} X + \varepsilon(p) p^{k-1}$ (respectivement $X^2 - \frac{a'_p}{p^{(k-1)/2}} X + \varepsilon'(p)^{k-1}$). En particulier, les racines locales en p de π et π' sont distinctes si, et seulement si, $a_p \neq a'_p$ ou $\varepsilon(p) \neq \varepsilon'(p)$. □

À la manière de ce qu'on avait fait pour les corps de fonctions, on souhaite calculer une borne optimale théorique sur le nombre de coefficients des q-développements de deux formes modulaires pour les différencier. On considère pour cela une forme primitive $f = \sum a_n q^n$ propre, de poids k, et de niveau N. Et on suppose que f est entièrement déterminée par ses coefficients a_p pour $p \leq n$ premier.

Chacun des coefficients a_p est un entier algébrique de norme au plus $p^{\frac{k-1}{2}}$. Comme la connaissance des a_p ne peut pas contenir plus d'information que le choix de f parmi les $s_k^{new}(N)$ formes primitives de poids k et niveau N, on en déduit que l'on a nécessairement l'inégalité :

$$\left(\prod_{p \leq n \text{ premier}} p \right)^{\frac{k-1}{2}} \geq s_k^{new}(N)$$

Et en passant au log :

$$\frac{k-1}{2} \log \left(\prod_{p \leq n \text{ premier}} p \right) \geq \log \left(s_k^{new}(N) \right). \tag{8}$$

On peut en dire un peu plus sur le membre de gauche de l'inégalité 8. On a l'équivalence $\log\left(\prod_{p\leq n \text{ premier}} p\right) \underset{n\to\infty}{\sim} n$, qui est une conséquence du théorème des nombres premiers. On montrera dans la suite que, pour les cas qui nous intéressent, on aura que n tend vers l'infini, et que l'on pourra donc utiliser cet équivalent.

Fixons k, et faisons varier N en le faisant tendre vers l'infini. Suivant les inégalités de (7), on a l'équivalence : $\log(s_k(N)) \underset{N\to\infty}{\sim} 3\log(N)$.

On en déduit donc que la quantité $\log(s_k^{new}(N))$ tend vers l'infini, et donc que la quantité $\log\left(\prod_{p\leq n \text{ premier}} p\right)$ aussi. Et finalement, n tend vers l'infini, ce qui était nécessaire pour l'utilisation du théorème des nombres premiers.

On peut donc utiliser l'équivalent précédent, et n doit vérifier l'inégalité :

$$n \geq \log(N)$$

à une constante multiplicative près qui dépend de k.

Finalement, l'écart entre la borne donnée par le théorème 3.1 et la borne optimale théorique précédente se quantifie de la façon suivante. Fixons k, et faisons tendre N vers l'infini. À des constantes multiplicatives près, qui dépendent de k : $\log^2(N)$ coefficients du q-développement sont suffisants pour distinguer des formes modulaires de poids k et de niveau N, tandis que $\log(N)$ sont nécessaires.

Fixons maintenant N, et faisons tendre k vers l'infini, et regardons ce que devient cette borne optimale théorique. Suivant les inégalités de 7, on a alors : $\log(s_k^{new}(N)) \underset{k\to\infty}{\sim} \log(k)$.

L'inégalité 8 est alors vérifiée dès lors que $n \geq 2$. Autrement dit, il faut au moins un coefficient du q-développement d'une forme modulaire pour la déterminer. Ce résultat laisse penser que, à niveau N fixé et pour k suffisamment grand, il suffit d'un nombre constant de coefficients du q-développement pour déterminer une forme modulaire propre de poids k et de niveau N.

Cette dernière observation va dans le sens d'une conjecture de Chow–Ghitza [3, Conjecture 4.1], que l'on rappelle ici :

Conjecture 4.2. *Soient $N, k \in \mathbb{N}^*$. On note $n_0 = n_0(N,k)$ le plus petit entier tel que, étant données $f = \sum a_n q^n, f' = \sum a'_n q^n$ deux formes modulaires propres paraboliques normalisées de poids k et niveau N, on a l'équivalence :*

$$f = g \Leftrightarrow (\forall\, n \leq n_0)\ a_n = a'_n.$$

Alors il existe une constante $K > 0$, dépendant de N, tel que : si $k > K$, alors n_0 est le plus petit nombre premier ne divisant pas N.

On donne ci-dessous le résultat plus faible, démontré par Chow–Ghitza [3, Theorem 4.4], et qui va dans le sens de la remarque précédente :

Théorème 4.3. *Avec les mêmes notations, si $k \geq 38$ est pair, alors n_0 est supérieur ou égal au plus petit nombre premier ne divisant pas N.*

Terminons par une comparaison entre notre borne théorique, et le résultat suivant dû à Sturm [16] :

Théorème 4.4. *Soient $N, k \in \mathbb{N}^*$, et $f = \sum a_n q^n, f' = \sum a'_n q^n$ deux formes modulaires normalisées de poids k et de niveau N distinctes. Alors il existe un entier n avec :*

$$n \leq \frac{k}{12}\,[\mathrm{SL}_2(\mathbb{Z}) : \Gamma(N)]$$

tel que $a_n \neq a'_n$.

Il y a principalement deux intérêts à utiliser le théorème 4.4 plutôt que le théorème 4.1. Déjà, la valeur de la constante C_{Euv} est trop grande pour rendre ce théorème applicable pour des petites valeurs de k et N. Ensuite, le théorème 4.1 nécessite que GRH soit vérifiée pour certaines fonctions L.

L'écart entre la borne donnée par le théorème 4.4 et la borne optimale théorique se quantifie de la manière suivante.

Si l'on fixe k, et que l'on fait tendre N vers l'infini, à des constantes multiplicatives près dépendant de k, N^3 coefficients du q-développement sont suffisants pour distinguer des formes modulaires de poids k et de niveau N, tandis que $\log(N)$ sont nécessaires.

Si l'on fixe N, et que l'on fait tendre k vers l'infini, à des constantes multiplicatives près dépendant de N, k coefficients du q-développement sont suffisants pour distinguer des formes modulaires de poids k et de niveau N, tandis qu'un nombre constant de coefficients sont nécessaires.

Dans ce dernier cas, si la conjecture de Chow–Ghitza était vérifiée, le nombre constant de coefficients à calculer serait le nombre de nombres premiers inférieurs ou égaux au plus petit nombre premier ne divisant pas N.

Références

[1] Arthur, *The endoscopic classification of representations : orthogonal and symplectic groups*, Colloquium Publ. 61, Amer. Math. Soc. (2013).

[2] Chenevier et Renard, *Level one algebraic cusp forms of classical groups of small rank*, Mem. Amer Math. Soc. 1121, 128p (2015).

[3] Chow et Ghitza, *Distinguishing newforms*, disponible à l'url http://arxiv.org/abs/1404.4508 (2018).

[4] Deligne, *La conjecture de Weil : I*, Publications mathématiques de l'IHES 43, p. 273-307 (1974).

[5] Deligne, *La conjecture de Weil : II*, Publications mathématiques de l'IHES 56, p. 137-252 (1980).

[6] Deligne, *Finitude de l'extension de $\mathbb{Q}$ engendrée par des traces de Frobenius, en caractéristique finie*, Moscow Math. Journal.

[7] Deligne et Flicker, *Counting local systems with principal unipotent local monodromy.*

[8] Esnault et Kerz, *A finiteness theorem for Galois representation of function fields over finite fields (after Deligne)*, Acta Math. Vietnam.

[9] Euvrard, *Majoration explicite sur le nombre de coefficients suffisants pour déterminer une fonction L*, Journal de théorie des nombres de Bordeaux, 29 no. 1 (2017), p. 51-83, doi : 10.5802/jtnb.969

[10] Iwaniec et Kowalski, *Analytic Number Theory*, American Mathematical Society, Vol. 53.

[11] Jacquet, Piateski-Shapiro et Shalika, *Conducteur des représentations du groupe linéaire*, Math. Annales 256(2), p. 199-214 (1981).

[12] Jacquet et Shalika, *On Euler products and the classification of automorphic representations*, Amer. J. Math. I : 103 (1981), 499-588 ; II : 103 (1981), 777-815.

[13] Laumon, *Transformation de Fourier, constantes d'équations fonctionnelles et conjectures de Weil*, Publications mathématiques de l'IHES 65, p. 131-210 (1987).

[14] Mégarbané, *Traces des opérateurs de Hecke sur les espaces de formes automorphes de* SO_7*,* SO_8 *ou* SO_9 *en niveau* 1 *et poids arbitraire*, à paraître dans le Journal de Théorie des Nombres de Bordeaux (2017)

[15] Moeglin et Waldspurger, *Stabilisation de la formule des traces tordue VI & X*, prépublications disponibles à l'url http://webusers.imj-prg.fr/~jean-loup.waldspurger/ (2014).

[16] Sturm, *On the congruence of modular forms* dans *Number Theory, New York*, 1984–85, Lect. Notes in Math.,1240, Springer-Verlag, 1987, Berlin, pp. 275–280.

[17] Waldspurger, *Stabilisation de la formule des traces tordues I, II, III, IV, V, VII, VIII, IX*, prépublications disponibles à l'url http://webusers.imj-prg.fr/~jean-loup.waldspurger/ (2014).

Université Grenoble Alpes, Institut Fourier, CNRS UMR 5582, 100 rue des Maths, 38610 Gières, France

E-mail address: thomas.megarbane@univ-grenoble-alpes.fr