Functiones et Approximatio
54.2 (2016), 195–226
doi: 10.7169/facm/2016.54.2.5

THE AMPLIFICATION METHOD IN THE CONTEXT OF $GL(n)$ AUTOMORPHIC FORMS

Guillaume Ricotta

Abstract: In [SV] and [BMb], the authors proved the existence of a so-called higher rank amplifier and in [HRRa], the authors described an explicit version of a $GL(3)$ amplifier. This article provides, for $n \geqslant 4$, a totally explicit $GL(n)$ amplifier and gives all the results required to use it effectively.

Keywords: amplification method, Hecke operators, Hecke algebras.

1. Introduction and statement of the results

1.1. Motivation

The general philosophy of the amplification method

The amplification method was set up by W. Duke, J. Friedlander and H. Iwaniec (see [FI92], [Iwa92] and [DFI94] for example).

When bounding say a complex number z, which satisfies for obvious reasons depending on the context

$$|z| \leqslant M \tag{1.1}$$

for some positive real number M but, which is expected to satisfy

$$|z| \leqslant M^{1-\delta} \tag{1.2}$$

for some $0 < \delta < 1$, it is sometimes profitable to include z in a finite family[1] of complex numbers of the same nature, say

$$z = z_{j_0} \in \{z_j, j \in J\} \coloneqq \mathcal{Z}_J$$

2010 Mathematics Subject Classification: primary: 11F99, 20C08; secondary: 15A21

[1] Note that choosing a family containing z may be highly non-trivial. In particular, it should be large enough in order to be able to use the powerful tools of harmonic analysis but not too large such that bounding a moment of small order, like the second one, has a chance to be successful.

where J is a finite set of cardinality $\asymp M$, $j_0 \in J$ is the index of our favourite complex number z and to estimate all the quantities occuring in this family on average.

For instance, one can try to bound the second moment of this family given by

$$M_2\left(\mathcal{Z}_J\right) := \sum_{j\in J} |z_j|^2.$$

By (1.1), the second moment satisfies

$$M_2\left(\mathcal{Z}_J\right) \leqslant |J| M^2,$$

which does not help us to prove (1.2) by positivity.

One can try to bound instead an amplified second moment given by

$$\mathcal{M}_2\left(\mathcal{Z}_J, \overrightarrow{\alpha}\right) := \sum_{j\in J} \left|M_j(\overrightarrow{\alpha})\right|^2 |z_j|^2$$

where $M_j\left(\overrightarrow{\alpha}\right)$ is a short Dirichlet polynomial given by

$$M_j\left(\overrightarrow{\alpha}\right) := \sum_{i\in I} \alpha_i a_j(i)$$

for $j \in J$ and where I is a small finite set. Here, $\overrightarrow{\alpha} = (\alpha_i)_{i\in I}$ is a finite sequence of complex numbers, which will be specified later on, and $(a_j(i))_{i\in I}$ are some complex numbers naturally related to z_j for $j \in J$. In practice, the currently known techniques enable us to prove

$$\mathcal{M}_2\left(\mathcal{Z}_J, \overrightarrow{\alpha}\right) \leqslant M^{\varepsilon}\left(M^2 ||\overrightarrow{\alpha}||_2^2 + |I|^{\beta} ||\overrightarrow{\alpha}||_1\right) \tag{1.3}$$

for some possibly large $\beta > 0$ and for all $\varepsilon > 0$, where as usual $||\overrightarrow{\alpha}||_1$ and $||\overrightarrow{\alpha}||_2$ stand for the L^1 and L^2 norms of $\overrightarrow{\alpha}$, respectively.

The whole point of the amplification method is to choose a sequence $\overrightarrow{\alpha}$, which amplifies the contribution of the complex number z in the amplified second moment $\mathcal{M}_2\left(\mathcal{Z}_J, \overrightarrow{\alpha}\right)$. More explicitely, one has to construct a sequence $\overrightarrow{\alpha}$ satisfying[2]

$$||\overrightarrow{\alpha}||_2 \leqslant |I|^{\varepsilon}, \qquad \left|M_{j_0}\left(\overrightarrow{\alpha}\right)\right|^2 \geqslant |I|^{\gamma}$$

for some possibly small $\gamma > 0$ and for all $\varepsilon > 0$. In general, cooking such sequence $\overrightarrow{\alpha}$ is based on the fact that some of the complex numbers $a_{j_0}(i)$, $i \in I$, cannot be small simultaneously. For such sequence, (1.3) entails by positivity

$$|z|^2 = |z_{j_0}|^2 \leqslant (M|I|)^{\varepsilon}\left(\frac{M^2}{|I|^{\gamma}} + |I|^{\beta+1/2-\gamma}\right) \tag{1.4}$$

for all $\varepsilon > 0$, which implies (1.2) by an optimal choice of $|I|$.

[2]Obviously one should also expect that $\left|M_j\left(\overrightarrow{\alpha}\right)\right|^2$ is not too large when $j \neq j_0$ in J for the amplification method to be successful. This generally follows in concrete cases, at least conditionally, from a suitable version of the Riemann Hypothesis. Hopefully, one does not this in practice.

The very natural first step towards the proof of (1.3) is to open the square and to switch the order of summation, which leads us to bounding

$$\sum_{(i_1,i_2)\in I^2} \alpha_{i_1}\overline{\alpha_{i_2}} \sum_{j\in J} a_j(i_1)\overline{a_j(i_2)}|z_j|^2. \tag{1.5}$$

The diagonal term, namely the contribution from $i_1 = i_2$ in (1.5), is generally bounded by the first term in the right-hand side of (1.4), whereas the non-diagonal term, namely the contribution from $i_1 \neq i_2$ in (1.5), is generally bounded by the second term in the right-hand side of (1.4).

Getting these bounds heavily relies in practice on linearising the products $a_j(i_1)\overline{a_j(i_2)}$ for i_1 and i_2 in I, namely these products can be often written in relevant cases as a linear combination of the $a_j(i)$'s. Such linearisations in the context of $GL(n)$ automorphic forms are the core of this article.

In practice, the complex numbers $a_j(i)$ and $\overline{a_j(i)}$, $(i,j) \in I \times J$, are the eigenfunctions of some specific endomorphisms. Thus, linearising the products $a_j(i_1)\overline{a_j(i_2)}$ boils down to linearising the composition of the relevant endomorphisms.

The amplification method in $GL(n)$

Let p and q be two prime numbers.

In the context of $GL(n)$ automorphic forms defined in Section 2, our favourite complex number z is related to a $GL(n)$ Hecke-Maaß cusp form f, say $z = z(f)$. For instance, $z = f(g)$ for g in the generalised upper-half plane or $z = L(f,s)$, the value of the Godement-Jacquet L-function attached to f on the critical line $\mathrm{Re}\,(s) = 1/2$.

Hence z can be included, with a slight abuse of notations, in a finite subset of an orthonormal basis $(f_j)_{j\geqslant 1}$ of $GL(n)$ Hecke-Maaß cusp forms, namely those whose analytic conductors, the Laplace eigenvalue or the level or the imaginary part of s for instance, is bounded by some parameter $Q > 0$, which is devoted to tend to infinity, say

$$z(f) = z(f_{j_0}) \in \{z(f_j), j \geqslant 1, Q(f_j) \leqslant Q\}.$$

In [SV], the authors proved the existence of an abstract higher rank amplifier and in [BMb], the authors proved that there exists, at least asymptotically (p large), a non-trivial linear combination of $GL(n)$ Hecke operators equal to the identity operator (see [BMb, Lemma 4.2]). The whole point of this work is to give a totally explicit and ready to use version of a $GL(n)$ amplifier.

The choice of our amplifier $\overrightarrow{\alpha}$ relies on the fundamental identity

$$a_{j_0}(p, \underbrace{1,\ldots,1}_{n-2 \text{ terms}})a_{j_0}(\underbrace{1,\ldots,1}_{n-2 \text{ terms}}, p) = a_{j_0}(p, \underbrace{1,\ldots,1}_{n-3 \text{ terms}}, p) + 1,$$

where $a_j(m_1,\ldots,m_{n-1})$ stands for the $(m_1,\ldots,m_{n-1})$'th Fourier coefficient of f_j (see (2.1) and [Gol06, Theorem 9.3.11, p. 271]). This identity essentially says that

$a_{j_0}(p,\underbrace{1,\dots,1}_{n-2\text{ terms}})a_{j_0}(\underbrace{1,\dots,1}_{n-2\text{ terms}},p)$ and $a_{j_0}(p,\underbrace{1,\dots,1}_{n-2\text{ terms}},p)$ cannot be simultaneously small . At the level of Hecke operators, this identity reflects the fact that

$$T_{\mathrm{diag}(1,\underbrace{p,\dots,p}_{n-1\text{ terms}})}\circ T_{\mathrm{diag}(\underbrace{1,\dots,1}_{n-1\text{ terms}},p)}=T_{\mathrm{diag}(1,\underbrace{p,\dots,p}_{n-2\text{ terms}},p^2)}+\frac{p^n-1}{p-1}\mathrm{Id},\tag{1.6}$$

itself a consequence of the identity

$$\begin{aligned}\Lambda_n\mathrm{diag}\left(\underbrace{1,\dots,1}_{n-1\text{ terms}},p\right)\Lambda_n*\Lambda_n\mathrm{diag}\left(1,\underbrace{p,\dots,p}_{n-1\text{ terms}}\right)\Lambda_n\\=\Lambda_n\mathrm{diag}\left(1,\underbrace{p,\dots,p}_{n-2\text{ terms}},p^2\right)\Lambda_n+\frac{p^n-1}{p-1}\Lambda_n\mathrm{diag}\left(\underbrace{p,\dots,p}_{n\text{ terms}}\right)\Lambda_n\end{aligned}$$

at the level of Λ_n double cosets, where $\Lambda_n:=GL_n(\mathbb{Z})$ (see [AZ95, Lemma 2.18, p. 114]).

The coefficients $a_j(i)$'th will be some Hecke eigenvalues of f_j. More precisely, being inspired by [HRRa] and by (1.6), we set

$$\begin{aligned}a_j(p)&:=a_j(p,\underbrace{1,\dots,1}_{n-1\text{ terms}})=\text{the eigenvalue of }T_p=p^{-(n-1)/2}T_{\mathrm{diag}(\underbrace{1,\dots,1}_{n-1\text{ terms}},p)},\\a_j\left(p^2\right)&:=\text{the eigenvalue of }p^{-(n-1)}T_{\mathrm{diag}(1,\underbrace{p,\dots,p}_{n-2\text{ terms}},p^2)}\in\mathbb{R}\end{aligned}$$

when acting on f_j and we recall that

$$\overline{a_j(p)}=\text{the eigenvalue of }T_p^*=p^{-(n-1)/2}T_{\mathrm{diag}(1,\underbrace{p,\dots,p}_{n-1\text{ terms}})}$$

still when acting on f_j (see (2.4)). Thus, I is a subset of the prime numbers and of the squares of the prime numbers.

A very natural candidate for a $GL(n)$ amplifier is

$$M_j\left(\overrightarrow{\alpha}\right):=\sum_{i\in I}\alpha_i a_j(i)$$

where

$$\alpha_i:=\begin{cases}\overline{a_{j_0}(p)} & \text{if } i=p\leqslant\sqrt{L}\text{ is a prime number,}\\-1 & \text{if } i=p^2\leqslant L\text{ is the square of a prime number}\\0 & \text{otherwise.}\end{cases}$$

This amplifier satisfies, as in the $GL(2)$ and $GL(3)$ case, $|M_{j_0}\left(\overrightarrow{\alpha}\right)|^2\gg_\varepsilon L^{1-\varepsilon}$ since $|I|\gg_\varepsilon L^{1-\varepsilon}$ for all $\varepsilon>0$.

Glancing at (1.5) and applying the inequality[3]

$$|M_{j_0}(\overrightarrow{\alpha})|^2 \leqslant 2\left|\sum_{p\leqslant\sqrt{L}} \alpha_p a_j(p)\right|^2 + 2\left|\sum_{p\leqslant\sqrt{L}} \alpha_{p^2} a_j(p^2)\right|^2,$$

it becomes crucial to linearise the products

$$T_{\mathrm{diag}(1,\underbrace{p,\ldots,p}_{n-1 \text{ terms}})} \circ T_{\mathrm{diag}(\underbrace{1,\ldots,1}_{n-1 \text{ terms}},q)} \text{ and } T_{\mathrm{diag}(1,\underbrace{p,\ldots,p}_{n-2 \text{ terms}},p^2)} \circ T_{\mathrm{diag}(1,\underbrace{q,\ldots,q}_{n-2 \text{ terms}},q^2)}$$

where p and q are two prime numbers. The results are given in the next section and reveal that the relevant Hecke operators when applying the amplification method in $GL(n)$ are

$$T_{\mathrm{diag}(1,\underbrace{p,\ldots,p}_{n-2 \text{ terms}},pq)}, \qquad T_{\mathrm{diag}(1,\underbrace{pq,\ldots,pq}_{n-2 \text{ terms}},(pq)^2)}, \qquad T_{\mathrm{diag}(1,\underbrace{p,\ldots,p}_{n-2 \text{ terms}},p^2)}$$

and

$$T_{\mathrm{diag}(1,\underbrace{p^2,\ldots,p^2}_{n-3 \text{ terms}},p^3,p^3)}, \qquad T_{\mathrm{diag}(1,1,\underbrace{p,\ldots,p}_{n-3 \text{ terms}},p^3)}, \qquad T_{\mathrm{diag}(1,1,\underbrace{p,\ldots,p}_{n-4 \text{ terms}},p^2,p^2)}.$$

1.2. Statement of the results

Theorem A. *Let $n \geqslant 4$, $\Lambda_n = GL_n(\mathbb{Z})$ and p be a prime number.*

1. *The finite set $R^{(n)}(p)$ of cardinality*

$$\deg\left(\mathrm{diag}\left(1, \underbrace{p,\ldots,p}_{n-2 \text{ terms}}, p^2\right)\right) = p\frac{\left(p^{n-1}-1\right)\left(p^n-1\right)}{(p-1)^2}$$

defined in Proposition 3.1 is a complete system of representatives of the distinct Λ_n right cosets of

$$\Lambda_n \mathrm{diag}\left(1, \underbrace{p,\ldots,p}_{n-2 \text{ terms}}, p^2\right)\Lambda_n$$

modulo Λ_n.

2. *The following formulas for the degrees[4] hold:*

$$\deg\left(\mathrm{diag}\left(p, \underbrace{p^2,\ldots,p^2}_{n-2 \text{ terms}}, p^3\right)\right) = p\frac{\left(p^{n-1}-1\right)\left(p^n-1\right)}{(p-1)^2}, \tag{1.7}$$

[3]Such inequality, used for the first time in the amplification method in [BHM], enabled the authors to avoid mixing squares of prime numbers and prime numbers in their diophantine analysis.

[4]The degree of a matrix is defined in (1.16). See also Section 2 for more details.

$$\deg\left(\operatorname{diag}\left(1,\underbrace{p^2,\ldots,p^2}_{n-3\text{ terms}},p^3,p^3\right)\right)=p^{n+1}\frac{\left(p^{n-2}-1\right)\left(p^{n-1}-1\right)\left(p^n-1\right)}{(p-1)^2(p^2-1)},\tag{1.8}$$

$$\deg\left(\operatorname{diag}\left(1,\underbrace{p^2,\ldots,p^2}_{n-2\text{ terms}},p^4\right)\right)=p^{2n-1}\frac{\left(p^{n-1}-1\right)\left(p^n-1\right)}{(p-1)^2},\tag{1.9}$$

$$\deg\left(\operatorname{diag}\left(p,p,\underbrace{p^2,\ldots,p^2}_{n-3\text{ terms}},p^4\right)\right)=p^{n+1}\frac{\left(p^{n-2}-1\right)\left(p^{n-1}-1\right)\left(p^n-1\right)}{(p-1)^2(p^2-1)},\tag{1.10}$$

and

$$\begin{aligned}\deg&\left(\operatorname{diag}\left(p,p,\underbrace{p^2,\ldots,p^2}_{n-4\text{ terms}},p^3,p^3\right)\right)\\&=p^4\frac{\left(p^{n-3}-1\right)\left(p^{n-2}-1\right)\left(p^{n-1}-1\right)\left(p^n-1\right)}{(p-1)^2\left(p^2-1\right)^2}.\end{aligned}\tag{1.11}$$

3. *Finally,*

$$\begin{aligned}&\Lambda_n\operatorname{diag}\left(1,\underbrace{p,\ldots,p}_{n-2\text{ terms}},p^2\right)\Lambda_n*\Lambda_n\operatorname{diag}\left(1,\underbrace{p,\ldots,p}_{n-2\text{ terms}},p^2\right)\Lambda_n\\
&\quad=\frac{2p^n-p^2-2p+1}{p-1}\Lambda_n\operatorname{diag}\left(p,\underbrace{p^2,\ldots,p^2}_{n-2\text{ terms}},p^3\right)\Lambda_n\\
&\quad\quad+p\frac{\left(p^{n-1}-1\right)\left(p^n-1\right)}{(p-1)^2}\Lambda_n\operatorname{diag}\left(\underbrace{p^2,\ldots,p^2}_{n\text{ terms}}\right)\Lambda_n\\
&\quad\quad+\Lambda_n\operatorname{diag}\left(1,\underbrace{p^2,\ldots,p^2}_{n-2\text{ terms}},p^4\right)\Lambda_n\\
&\quad\quad+(p+1)\Lambda_n\operatorname{diag}\left(1,\underbrace{p^2,\ldots,p^2}_{n-3\text{ terms}},p^3,p^3\right)\Lambda_n\\
&\quad\quad+(p+1)\Lambda_n\operatorname{diag}\left(p,p,\underbrace{p^2,\ldots,p^2}_{n-3\text{ terms}},p^4\right)\Lambda_n\\
&\quad\quad+(p+1)^2\Lambda_n\operatorname{diag}\left(p,p,\underbrace{p^2,\ldots,p^2}_{n-4\text{ terms}},p^3,p^3\right)\Lambda_n.\end{aligned}\tag{1.12}$$

Corollary B. *Let $n \geqslant 4$. If p and q are two prime numbers then*

$$T_{\mathrm{diag}(1,\underbrace{p,\ldots,p}_{n-1 \text{ terms}})} \circ T_{\mathrm{diag}(\underbrace{1,\ldots,1}_{n-1 \text{ terms}},q)} = T_{\mathrm{diag}(1,\underbrace{p,\ldots,p}_{n-2 \text{ terms}},pq)} + \delta_{p=q}\frac{p^n-1}{p-1}\mathrm{Id} \tag{1.13}$$

and

$$\begin{aligned} &T_{\mathrm{diag}(1,\underbrace{p,\ldots,p}_{n-2 \text{ terms}},p^2)} \circ T_{\mathrm{diag}(1,\underbrace{q,\ldots,q}_{n-2 \text{ terms}},q^2)} \\ &\quad = T_{\mathrm{diag}(1,\underbrace{pq,\ldots,pq}_{n-2 \text{ terms}},(pq)^2)} + \delta_{p=q}\frac{2p^n-p^2-2p+1}{p-1}T_{\mathrm{diag}(1,\underbrace{p,\ldots,p}_{n-2 \text{ terms}},p^2)} \\ &\quad + \delta_{p=q}p\frac{\left(p^{n-1}-1\right)\left(p^n-1\right)}{(p-1)^2}\mathrm{Id} + \delta_{p=q}(p+1)T_{\mathrm{diag}(1,\underbrace{p^2,\ldots,p^2}_{n-3 \text{ terms}},p^3,p^3)} \\ &\quad + \delta_{p=q}(p+1)T_{\mathrm{diag}(1,1,\underbrace{p,\ldots,p}_{n-3 \text{ terms}},p^3)} + \delta_{p=q}(p+1)^2T_{\mathrm{diag}(1,1,\underbrace{p,\ldots,p}_{n-4 \text{ terms}},p^2,p^2)}. \end{aligned} \tag{1.14}$$

When $p \neq q$, the previous corollary follows from (2.13) whereas when $p = q$, it comes from Theorem A, [AZ95, Lemma 2.18, p. 114] and (2.9). This corollary generalizes the case $n = 2$, well-known for a long time, and the case $n = 3$ done in [HRRa].

1.3. On the possible applications of this higher rank amplifier

Subconvexity bounds for L-functions

Let f be a $GL(n)$ Hecke Maaß cusp form. A very classical problem considered by analytic number theorists is the size of the Godement-Jacquet L-function associated to f, say $L(f,s)$ with s on the critical line $\mathrm{Re}\,(s) = 1/2$ when the analytic conductor $C(f)$ of f tends to infinity. The bound

$$L(f,s) \ll C(f)^{1/4+\varepsilon},$$

for any $\varepsilon > 0$ is named the convexity or trivial bound, even if this is not a trivial result in general. Improving this bound, namely proving a subconvexity bound, was proved in the past to be useful to solve many arithmetical questions, such as equidistribution results.

The $GL(2)$ case was intensively investigated in the last decades, culminating in the work of P. Michel and A. Venkatesh in [MV10], who used the amplification method in $GL(2)$. It seems that the best subconvexity bounds in the $GL(2)$ case intrinsic to the amplification method are the Weyl exponent $1/4(1-1/3)$ ([Wey21]) and the Burgess exponent $1/4(1-1/4)$ ([Bur62]).

Very few examples of subconvexity bounds for L-functions of $GL(n)$ automorphic forms, which are not lifts of $GL(2)$ ones, are known. One can quote [Li11], [Blo12], [Muna], [BB] in the rank 2 case, and an extremely recent and elaborate subconvexity bound for twisted L-functions of $GL(3)$ automorphic forms by R. Munshi in [Munb]. As far as we know, the Weyl and Burgess exponents have never appeared in this higher rank case.

We hope that the completely explicit $GL(n)$ amplifier built in this paper will sheld some new lights on these questions in the close future.

Subconvexity bounds for sup-norms of automorphic forms

Let f be a L^2-normalized $GL(n)$ Hecke-Maaß cusp form.

The spectral aspect. Let K be a fixed compact subset of $SL_n(\mathbb{R})/SO_n(\mathbb{R})$. The convexity bound for the sup-norm of f restricted to K is given by

$$||f|_K||_\infty \ll \lambda_f^{n(n-1)/8}$$

where λ_f is the Laplace eigenvalue of f. More details can be found in [Sar]. It is important to mention that F. Brumley and N. Templier discovered in [BT] that this convexity bound does not hold when $n \geqslant 6$ if f is not restricted to a compact.

The convexity bound is not expected to be sharp, essentially because there are some additional symmetries on $SL_n(\mathbb{R})/SO_n(\mathbb{R})$: the Hecke correspondences. More precisely, one should be able to prove a subconvexity bound, namely finding an absolute positive constant $\delta_n > 0$ such that

$$||f|_K||_\infty \ll \lambda_f^{n(n-1)/8-\delta_n} \tag{1.15}$$

The pioneering work done by H. Iwaniec and P. Sarnak in [IS95] is the bound given in (1.15) when $n = 2$ for $\delta_2 = 1/24$. This constant δ_2 seems to be intrinsic to the amplification method in $GL(2)$. The case $n = 3$ was completed in [HRRb]. The general case was done in a series of impressive works by V. Blomer and P. Maga in [BMb] and in [BMa]. One could also quote [Marb].

All these achievements were done thanks to the amplification method. Determining what should be the best subconvexity exponent intrinsic to the amplification method is an interesting question, which should reveal new types of analytic problems. Needless to say that the explicit $GL(n)$ amplifier could be useful to do so.

The level aspect. Let us say that f is of level q and let us speak about the growth of the sup-norm of f as q gets large.

For $GL(2)$ and when the level q is squarefree, the convexity bound is

$$||f||_\infty \ll q^\varepsilon$$

for all $\varepsilon > 0$ but one expects that the correct order of magnitude is

$$||f||_\infty \ll q^{-1/2+\varepsilon}$$

This rank 1 case in prime level was intensively studied during the last years after the foundational work of V. Blomer and R. Holowinsky in [BH10], particularly in [Tem10], [HT12] and [HR]. In [HT13], the authors proved the bound

$$||f||_\infty \ll q^{-1/6+\varepsilon}$$

which seems to be the best possible subconvexity exponent intrinsic to the amplification method. Note that the authors really used the **shape** of the explicit $GL(2)$ amplifier in order to get this bound. When the level q is not squarefree, the situation is more delicate since the Atkin-Lehner group has more than one orbit when acting on the cusps. See [Sah] and [Mara] for more details.

For $GL(n)$, as far as we know, these questions remain completely open. We hope that the explicit $GL(n)$ amplifier constructed in this work will make possible an investigation of these questions in a higher rank setting.

1.4. Organization of the paper

The general background on $GL(n)$ Maaß cusp forms and on the $GL(n)$ Hecke algebra is given in Section 2. The proof of part (1) in Theorem A is done in Section 3 (see Proposition 3.1). The proofs of parts (2) and (3) in Theorem A are detailed in Section 4.

Notations. $n \geqslant 2$ is an integer and p, q are prime numbers. Λ_n stands for the group $GL_n(\mathbb{Z})$ of $n\times n$ invertible matrices with integer entries, whose unity element is the identity matrix I_n. For g a $n\times n$ matrix with rational coefficients, the degree of g is defined by

$$\deg(g) = \operatorname{card}\left(\Lambda_n \setminus \Lambda_n g \Lambda_n\right). \tag{1.16}$$

If $a_1, \ldots, a_n$ are real numbers then $\operatorname{diag}(a_1, \ldots, a_n)$ denotes the $n \times n$ diagonal matrix with $a_1, \ldots, a_n$ as diagonal entries. The following double Λ_n cosets will occur throughout this article:

$$\pi_i^{(n)}(p) \coloneqq \Lambda_n D_i^{(n)}(p) \Lambda_n, \qquad D_i^{(n)}(p) = \operatorname{diag}\left(1, \ldots, 1, \underbrace{p, \ldots, p}_{i\text{terms}}\right),$$

$$\pi^{(n)}(p) \coloneqq \Lambda_n D^{(n)}(p) \Lambda_n, \qquad D^{(n)}(p) = \operatorname{diag}\left(1, \underbrace{p, \ldots, p}_{n-2 \text{ terms}}, p^2\right),$$

$$\pi_{i,j}^{(n)}(p) \coloneqq \Lambda_n D_{i,j}^{(n)}(p) \Lambda_n, \qquad D_{i,j}^{(n)}(p) = \operatorname{diag}\left(1, \ldots, 1, \underbrace{p, \ldots, p}_{i\text{terms}}, \underbrace{p^2, \ldots, p^2}_{j \text{ terms}}\right)$$

for $0 \leqslant i, j \leqslant n$ with $i + j \leqslant n$. The following polynomials in x will occur when computing the degrees of some relevant Λ_n double cosets for this work:

$$\varphi_r(x) \coloneqq \prod_{k=1}^{r} \left(x^k - 1\right), \qquad \varphi_0(x) = 1$$

for $r \geqslant 1$. Let us define the n-tuple

$$\boldsymbol{d}_n(p) := \left(1, p, p^2, \ldots, \underbrace{p^{k-1}}_{k\text{'th term}}, \ldots, p^{n-2}, p^n\right).$$

Finally, if $\mathcal{P}$ is a property then $\delta_{\mathcal{P}}$ is the Kronecker symbol, namely 1 if $\mathcal{P}$ is satisfied and 0 otherwise.

Acknowledgements. The author heartily thanks the anonymous referee for her or his long list of constructive suggestions, which greatly improved both the presentation and the arguments in some proofs.

He would like to thank R. Holowinsky and E. Royer for fruitful discussions related to this work.

The author's research was partially supported by a Marie Curie Intra European Fellowship within the 7th European Community Framework Programme. The grant agreement number of this project, whose acronym is ANERAUTOHI, is PIEF-GA-2009-251271. He would like to thank E. Kowalski, ETH and its entire staff for the excellent working conditions.

Last but not least, he would like to express his gratitude to K. Belabas for his crucial but isolated support for Analytic Number Theory among the Number Theory research team A2X (Institut de Mathématiques de Bordeaux, Université de Bordeaux).

2. Background on the $GL(n)$ Hecke algebra

In this section, $n \geqslant 2$. The convenient references for this section are [AZ95], [Gol06], [Kri90], [New72] and [Shi94].

Let f be a $GL(n)$ Maaß cusp form of level 1. Such f admits a Fourier expansion

$$f(g) = \sum_{\gamma \in U_{n-1}(\mathbb{Z})\backslash SL_{n-1}(\mathbb{Z})} \sum_{\substack{m_1, \ldots, m_{n-2} \geqslant 1 \\ m_{n-1} \in \mathbb{Z}^*}} \frac{a_f(m_1, \ldots, m_{n-1})}{\prod_{1 \leqslant k \leqslant n-1} |m_k|^{k(n-k)/2}} \tag{2.1}$$
$$\times W_{\mathrm{Ja}}\left(\mathrm{diag}\left(m_1 \ldots m_{n-2}|m_{n-1}|, \ldots, m_1 m_2, m_1, 1\right)\begin{pmatrix} \gamma & \\ & 1 \end{pmatrix} g, \nu_f, \psi_{\underbrace{1, \ldots, 1}_{n-2 \text{ terms}}, \frac{m_{n-1}}{|m_{n-1}|}}\right)$$

for $g \in GL_n(\mathbb{R})$ (see [Gol06, Equation (9.1.2)]. Here $U_{n-1}(\mathbb{Z})$ stands for the $\mathbb{Z}$-points of the group of $(n-1) \times (n-1)$ upper-triangular unipotent matrices. $\nu_f \in \mathbb{C}^{n-1}$ is the type of f, whose components are complex numbers characterized by the property that, for every invariant differential operator D in the center of the universal enveloping algebra of $GL_n(\mathbb{R})$, the cusp form f is an eigenfunction of D with the same eigenvalue as the power function I_{ν_f}, which is defined in [Gol06, Equation (5.1.1)]. $\psi_{\underbrace{1, \ldots, 1}_{n-2 \text{ terms}}, \pm 1}$ is the character of the group of $n \times n$

upper-triangular unipotent real matrices defined by

$$\psi_{\underbrace{1,\ldots,1}_{n-2\text{ terms}},\pm1}(u)=e^{2i\pi(u_{1,2}+\cdots+u_{n-2,n-1}\pm u_{n-1,n})}.$$

for $u=[u_{i,j}]_{1\leqslant i,j\leqslant n}$. $W_{Ja}\left(*,\nu_f,\psi_{\underbrace{1,\ldots,1}_{n-2\text{ terms}},\pm1}\right)$ stands for the $GL(n)$ Jacquet Whittaker function of type ν_f and character $\psi_{\underbrace{1,\ldots,1}_{n-2\text{ terms}},\pm1}$ defined in [Gol06, Equation 6.1.2]. The complex number $a_f(m_1,\ldots,m_{n-1})$ is the $(m_1,\ldots,m_{n-1})$'th *Fourier coefficient* of f for $m_1,\ldots,m_{n-2}$ some positive integers and m_{n-1} a non-vanishing integer.

For $g\in GL_n(\mathbb{Q})$, one knows (see [AZ95, Lemma 1.2, p. 94 and Lemma 2.1, p. 105]) that the Λ_n double coset $\Lambda_n g\Lambda_n$ is a finite union of Λ_n right cosets such that it makes sense to define the *Hecke operator* T_g by

$$T_g(f)(h)=\sum_{\delta\in\Lambda_n\backslash\Lambda_n g\Lambda_n}f(\delta h)$$

for $h\in GL_n(\mathbb{R})$ (see [AZ95, Chapter 3, Sections 1.1 and 1.5]. The *degree* of g or T_g is defined by

$$\deg(g)=\deg(T_g)=\operatorname{card}\left(\Lambda_n\setminus\Lambda_n g\Lambda_n\right).$$

Obviously,

$$\deg(rg)=\deg(g). \tag{2.2}$$

for $r\in\mathbb{Q}^\times$. By [AZ95, Lemma 2.18 Equation (2.32), p. 114],

$$\deg\left(D_{i,j}^{(n)}(p)\right)=p^{j(n-i-j)}\frac{\varphi_n(p)}{\varphi_{n-i-j}(p)\varphi_i(p)\varphi_j(p)} \tag{2.3}$$

for $0\leqslant i,j\leqslant n$ with $i+j\leqslant n$.

Remark 2.1. The equations (2.2) and (2.3) prove (1.7) and (1.11) in Theorem A.

The adjoint of T_g for the Peterson inner product is $T_{g^{-1}}$. The algebra of Hecke operators $\mathbb{T}$ is the ring of endomorphisms generated by all the T_g's with $g\in GL_n(\mathbb{Q})$, a commutative algebra of normal endomorphisms (see [Gol06, Theorem 9.3.6]), which contains the m'th normalised Hecke operator

$$T_m=\frac{1}{m^{(n-1)/2}}\sum_{\substack{g=\mathrm{diag}(y_1,\ldots,y_n)\\ y_1|y_2|\cdots|y_n\\ y_1y_2\cdots y_n=m}}T_g$$

for all positive integer m. A *Hecke-Maaß cusp form* f of level 1 is a Maaß cusp form of level 1, which is an eigenfunction of $\mathbb{T}$. In particular, it satisfies

$$T_m(f)=a_f(m,\underbrace{1,\ldots,1}_{n-2\text{ terms}})f\text{ and }T_m^*(f)=a_f(\underbrace{1,\ldots,1}_{n-2\text{ terms}},m)f \tag{2.4}$$

according to [Gol06, Theorem 9.3.11].

The algebra $\mathbb{T}$ is isomorphic to the *absolute Hecke algebra*, the free $\mathbb{Z}$-module generated by the double cosets $\Lambda_n g \Lambda_n$ where g ranges over $\Lambda_n \setminus GL_n(\mathbb{Q})/\Lambda_n$ and endowed with the following multiplication law. If g_1 and g_2 belong to $GL_n(\mathbb{Q})$ and

$$\Lambda_n g_1 \Lambda_n = \bigcup_{i=1}^{\deg(g_1)} \Lambda_n \alpha_i \text{ and } \Lambda_n g_2 \Lambda_n = \bigcup_{j=1}^{\deg(g_2)} \Lambda_n \beta_j$$

then

$$\Lambda_n g_1 \Lambda_n * \Lambda_n g_2 \Lambda_n = \sum_{\Lambda_n h \Lambda_n \subset \Lambda_n g_1 \Lambda_n g_2 \Lambda_n} m(g_1, g_2; h) \Lambda_n h \Lambda_n \tag{2.5}$$

where $h \in GL_n(\mathbb{Q})$ ranges over a system of representatives of the Λ_n-double cosets contained in the set $\Lambda_n g_1 \Lambda_n g_2 \Lambda_n$ and

$$\begin{aligned} & m(g_1, g_2; h) \\ & \quad = \operatorname{card}\left(\{(i,j) \in \{1, \dots, \deg(g_1)\} \times \{1, \dots, \deg(g_2)\}, \alpha_i \beta_j \in \Lambda_n h\}\right), & (2.6) \\ & \quad = \frac{1}{\deg(h)} \operatorname{card}\left(\{(i,j) \in \{1, \dots, \deg(g_1)\} \times \{1, \dots, \deg(g_2)\}, \alpha_i \beta_j \in \Lambda_n h \Lambda_n\}\right), & (2.7) \\ & \quad = \frac{\deg(g_2)}{\deg(h)} \operatorname{card}\left(\{i \in \{1, \dots, \deg(g_1)\}, \alpha_i g_2 \in \Lambda_n h \Lambda_n\}\right) & (2.8) \end{aligned}$$

by [AZ95, Lemma 1.5, p. 96]. In particular,

$$\Lambda_n r I_n \Lambda_n * \Lambda_n g \Lambda_n = \Lambda_n r g \Lambda_n \tag{2.9}$$

for $g \in GL_n(\mathbb{Q})$ and $r \in \mathbb{Q}^\times$ ([AZ95, Lemma 2.4, p. 107]).

For $g \in GL_n(\mathbb{Q})$ with integer entries, the Λ_n right coset $\Lambda_n g$ contains a unique upper-triangular column reduced matrix, namely

$$\Lambda_n g = \Lambda_n C \tag{2.10}$$

where $C = [c_{i,j}]_{1 \leqslant i,j \leqslant n}$ is an upper-triangular matrix with integer entries satisfying

$$\forall j \in \{2, \dots, n\}, \forall i \in \{1, j-1\}, \quad 0 \leqslant c_{i,j} < c_{j,j}$$

by [AZ95, Lemma 2.7].

Let g be a $n \times n$ matrix with integer entries. Let $1 \leqslant k \leqslant n$. Let $I_{n,k}$ be the set of all k-tuples $\{i_1, \dots, i_n\}$ satisfying $1 \leqslant i_1 < i_2 < \dots < i_k \leqslant n$. Obviously, $I_{n,k}$ is of cardinal $\binom{n}{k}$. If ω and τ are two elements of $I_{n,k}$ then $g(\omega, \tau)$ will denote the $k \times k$ determinantal minor of g whose row indices are the elements of ω and whose column indices are the elements of τ. Obviously, there are $\binom{n}{k}^2$ such minors. The k'th *determinantal divisor* of g, say $d_k(g)$, is the non-negative integer defined by

$$d_k(g) = \begin{cases} 0 & \text{if } \forall (\omega, \tau) \in I_{n,k}^2, g(\omega, \tau) = 0, \\ gcd_{(\omega,\tau) \in I_{n,k}^2} g(\omega, \tau) & \text{otherwise} \end{cases} \tag{2.11}$$

and the *determinantal vector* of g is $\boldsymbol{d}_n(g)=(d_1(g),\ldots,d_n(g))$. The determinantal divisors turn out to be useful since if h is another $n\times n$ matrix with integer entries then

$$h\in\Lambda_n g\Lambda_n \qquad \text{if and only if} \qquad \boldsymbol{d}(h)=\boldsymbol{d}(g) \tag{2.12}$$

according to [New72].

By [AZ95, Proposition 2.5, p. 107], if g_1,g_2 belong to $GL_n(\mathbb{Q})$ with integer entries then

$$\Lambda_n g_1\Lambda_n * \Lambda_n g_2\Lambda_n=\Lambda_n g_1 g_2\Lambda_n \tag{2.13}$$

provided $d_1(g_1)=d_1(g_2)=1$ and $(d_n(g_1),d_n(g_2))=1$.

Finally, we will use the following result on the local integral Hecke algebra at the prime p, say $\underline{H}_p^n$, defined as the Λ_n double cosets $\Lambda_n g\Lambda_n$, where g ranges over the matrices in $GL_n\left(\mathbb{Z}[1/p]\right)$ with integer entries. By [AZ95, Lemma 2.16, p. 112], the $\mathbb{Q}$-linear map $\Psi:\underline{H}_p^n\to\underline{H}_p^{n-1}$ defined by

$$\begin{aligned}\Psi&\left(\Lambda_n\mathrm{diag}\left(p^{\delta_1},\ldots,p^{\delta_n}\right)\Lambda_n\right)\\ &=\begin{cases}\Lambda_n\mathrm{diag}\left(p^{\delta_2},\ldots,p^{\delta_n}\right)\Lambda_n & \text{if } 0=\delta_1\leqslant\delta_2\leqslant\ldots\leqslant\delta_n,\\ 0 & \text{otherwise}\end{cases}\end{aligned} \tag{2.14}$$

is a morphism of rings.

3. Decomposition of $\pi^{(n)}(p)$ into Λ_n right cosets

In this section, $n\geqslant 2$. The main purpose of this section is to prove part (1) in Therorem A, namely to find a convenient complete system of representatives for the distinct Λ_n right cosets of $\pi^{(n)}(p)$ modulo Λ_n. Let us denote by $R_0^{(n)}(p)$ the set of $n\times n$ upper-triangular matrices $C=[c_{i,j}]_{1\leqslant i,j\leqslant n}$ with integer entries satisfying

$$\boldsymbol{d}_n(C)=\boldsymbol{d}_n(p), \tag{3.1}$$

$$\forall i\in\{1,\ldots,n\}, \qquad c_{i,i}=p, \tag{3.2}$$

and

$$\forall j\in\{2,\ldots,n\},\forall i\in\{1,\ldots,j-1\}, \qquad 0\leqslant c_{i,j}<p. \tag{3.3}$$

Let us also denote by $R_1^{(n)}(p)$ the set of $n\times n$ upper-triangular matrices $C=[c_{i,j}]_{1\leqslant i,j\leqslant n}$ with integer entries satisfying

$$\forall i\in\{1,\ldots,n\}, \quad c_{i,i}\in\left\{1,p,p^2\right\}, \tag{3.4}$$

$$\exists! i\in\{1,\ldots,n\}, \quad c_{i,i}=1 \qquad\text{and}\qquad \exists! i\in\{1,\ldots,n\}, \quad c_{i,i}=p^2, \tag{3.5}$$

$$\forall j\in\{2,\ldots,n\},\forall i\in\{1,\ldots,j-1\}, \qquad 0\leqslant c_{i,j}<c_{j,j} \tag{3.6}$$

and

$$\forall i\in\{1,\ldots,n-1\},\ p\mid c_{i,i}\Rightarrow\forall j\in\{i+1,\ldots,n\},\ p\mid c_{i,j}. \tag{3.7}$$

Proposition 3.1. *Let $n \geqslant 2$. The set $R^{(n)}(p) = R_0^{(n)}(p) \sqcup R_1^{(n)}(p)$ is a complete system of representatives of the distinct Λ_n right cosets of $\pi^{(n)}(p)$ modulo Λ_n. In other words,*

$$\pi^{(n)}(p) = \left(\bigsqcup_{C_0 \in R_0^{(n)}(p)} \Lambda_n C_0 \right) \bigsqcup \left(\bigsqcup_{C_1 \in R_1^{(n)}(p)} \Lambda_n C_1 \right).$$

In addition,

$$\begin{aligned} card\left(R_0^{(n)}(p)\right) &= \frac{(n-1)p^n - np^{n-1} + 1}{p-1}, \\ card\left(R_1^{(n)}(p)\right) &= \frac{p^{2n} - np^{n+1} + 2(n-1)p^n - np^{n-1} + 1}{(p-1)^2}. \end{aligned}$$

Remark 3.2. Proposition 3.1 proves part (1) in Theorem A.

Proof of Proposition 3.1. By (3.7), all the matrices C_1 in $R_1^{(n)}(p)$ can be decomposed as

$$C_1 = \text{diag}\left(p^{\alpha_1}, \ldots, p^{\alpha_n}\right) C_1'$$

for some non negative integers $\alpha_1, \ldots, \alpha_n$ and with $C_1' \in \Lambda_n$, hence

$$C_1 \in \Lambda \text{diag}\left(p^{\alpha_1}, \ldots, p^{\alpha_n}\right) \Lambda = \pi^{(n)}(p)$$

by (3.4) and (3.5).

All the matrices C_0 in $R_0^{(n)}(p)$ belong to $\pi^{(n)}(p)$ since their determinantal vectors match the determinantal vector of $D^{(n)}(p)$ by (3.1).

All the matrices in $R^{(n)}(p)$ are upper-triangular column reduced matrices by (3.3), (3.6) and belong to different Λ_n right cosets according to the unicity statement given in (2.10).

Let $C = [c_{i,j}]_{1 \leqslant i,j \leqslant n}$ be any upper-triangular column reduced matrix that lies in $\pi^{(n)}(p)$ and let us prove that C belongs to $R^{(n)}(p)$. First of all, the determinant of C is p^n, hence

$$\forall i \in \{1, \ldots, n\}, \exists \alpha_i \in \mathbb{N}, \quad c_{i,i} = p^{\alpha_i}.$$

Then, $C = \lambda_1 D^{(n)}(p) \lambda_2$ with λ_1, λ_2 in Λ_n, which entails that $C^{-1} = \lambda_2^{-1} D^{(n)}(p)^{-1} \lambda_1^{-1}$. As a consequence, $p^2 C^{-1}$ has integer entries and

$$\forall i \in \{1, \ldots, n\}, \qquad \alpha_i \in \{0, 1, 2\}.$$

If all the diagonal entries of C are equal to p then C belongs to $R_0^{(n)}(p)$ since its determinantal vector must be equal to the determinantal vector of $D^{(n)}(p)$, namely $\boldsymbol{d}_n(p)$. Assume that one of its diagonal coefficient is not equal to p. The condition $d_2(C) = p$ implies that there must be at most one diagonal coefficient of C equal to 1. Let us prove that C has a single diagonal coefficient equal to 1 and a single coefficient equal to p^2. Let σ be the permutation of $\{1,\dots,n\}$ satisfying

$$0 \leqslant \alpha_{\sigma(1)} \leqslant \dots \leqslant \alpha_{\sigma(n)} \leqslant 2.$$

The determinant condition is

$$\alpha_{\sigma(1)} + \cdots + \alpha_{\sigma(n)} = n.$$

If $\alpha_{\sigma(1)} = 0$ then one easily gets $\alpha_{\sigma(2)} = \cdots = \alpha_{\sigma(n-1)} = 1$ and $\alpha_{\sigma(n)} = 2$. If $\alpha_{\sigma(1)} \geqslant 1$ then all the diagonal entries of C are equal to p, which is a contradiction. Thus, (3.5) is satisfied. Let us prove (3.7). Assume on the contrary that there exist i_0 in $\{1,\dots,n-1\}$ and j_0 in $\{i_0+1,\dots,n\}$ such that $p \mid c_{i_0,i_0}$ and $p \nmid c_{i_0,j_0}$. The fact that $p \nmid c_{i_0,j_0}$ implies that $c_{j_0,j_0} \neq 1$. Let $j_1 \neq j_0$ be the index of the column of C, for which $c_{j_1,j_1} = 1$. Let us prove that the columns $C[j_1]$ of C of index j_1 and $C[j_0]$ of C of index j_0 are linearly independent modulo p. If

$$0 = \lambda_0 C[j_0] + \lambda_1 C[j_1] \pmod{p}$$

then the i_0'th component implies that

$$0 = \lambda_0 c_{i_0,j_0} + \lambda_1 c_{i_0,j_1} = \lambda_0 c_{i_0,j_0} \pmod{p}$$

such that $\lambda_0 = 0 \pmod{p}$ since c_{i_0,j_0} is invertible modulo p and $\lambda_1 = 0 \pmod{p}$. This is a contradiction since C is of rank 1 modulo p. Thus, C belongs to $R_1^{(n)}(p)$.

Let us compute the cardinality of $R_1^{(n)}(p)$. Obviously,

$$\begin{aligned}
\operatorname{card}\left(R_1^{(n)}(p)\right) &= p^{n-1} \sum_{1 \leqslant \alpha_1 \neq \alpha_2 \leqslant n} p^{\alpha_2-\alpha_1} \\
&= \left(\sum_{0 \leqslant \alpha \leqslant n-1} p^{\alpha}\right)^2 - np^{n-1} \\
&= \frac{p^{2n} - np^{n+1} + 2(n-1)p^n - np^{n-1} + 1}{(p-1)^2}.
\end{aligned}$$

Let us compute the cardinality of $R_0^{(n)}(p)$. Obviously,

$$\begin{aligned}
\operatorname{card}\left(R_0^{(n)}(p)\right) &= \operatorname{card}\left(R^{(n)}(p)\right) - \operatorname{card}\left(R_1^{(n)}(p)\right) \\
&= \deg\left(D^{(n)}(p)\right) - \operatorname{card}\left(R_1^{(n)}(p)\right) \\
&= p\frac{\varphi_n(p)}{\varphi_1(p)^2\varphi_{n-2}(p)} - \frac{p^{2n} - np^{n+1} + 2(n-1)p^n - np^{n-1} + 1}{(p-1)^2} \\
&= p\frac{\left(p^{n-1}-1\right)\left(p^n-1\right)}{(p-1)^2} - \frac{p^{2n} - np^{n+1} + 2(n-1)p^n - np^{n-1} + 1}{(p-1)^2}
\end{aligned}$$

by (2.3), which is the expected result. ■

We will need more details, stated in the following proposition, on the matrices in $R_0^{(n)}(p)$.

Proposition 3.3. *Let $n \geqslant 4$ and $C_0 = [c_{i,j}]_{1\leqslant i,j\leqslant n} \in R_0^{(n)}(p)$. On the one hand, $C_0 \neq pI_n$. On the other hand, for all positive integers i, j, k, ℓ, one has*

$$1 \leqslant i < k < j < \ell \leqslant n \Rightarrow c_{i,j}c_{k,\ell} \equiv c_{i,\ell}c_{k,j} \pmod p$$
$$1 \leqslant i < j \leqslant k < \ell \leqslant n \Rightarrow c_{i,j}c_{k,\ell} = 0.$$

Remark 3.4. One can check that

$$R_0^{(2)}(p) = \bigsqcup_{0<c_{1,2}<p} \left\{ \begin{pmatrix} p & c_{1,2} \\ & p \end{pmatrix} \right\},$$

$$R_0^{(3)}(p) = \bigsqcup_{\substack{0\leqslant c_{1,2},c_{1,3},c_{2,3}<p \\ c_{1,2}c_{2,3}=0 \\ (c_{1,2},c_{1,3},c_{2,3})\neq(0,0,0)}} \left\{ \begin{pmatrix} p & c_{1,2} & c_{1,3} \\ & p & c_{2,3} \\ & & p \end{pmatrix} \right\}.$$

Proof of Proposition 3.3. The fact that $C_0 \neq pI_n$ is obvious since the first determinantal divisor of C_0, whose value is 1, is nothing else than the greatest common divisor of the entries of C_0, which are non-negative integers strictly less than p.

Recall that $d_2(C_0) = p$. As a consequence, p divides the determinantal minors of C_0 of size 2 given by

$$c_{i,j}c_{k,\ell} - c_{i,\ell}c_{k,j} \tag{3.8}$$

for all $1 \leqslant i < k < j < \ell \leqslant n$. It also divides the determinantal divisors of C_0 of size 2 given by

$$c_{i,j}c_{j,\ell} - c_{i,\ell}c_{j,j} = c_{i,j}c_{j,\ell} - pc_{i,\ell} \tag{3.9}$$

for $1 \leqslant i < j < \ell \leqslant n$. The fact that the prime number p divides $c_{i,j}c_{j,\ell}$implies that $c_{i,j}c_{j,\ell} = 0$ because the non-diagonal entries of C_0 are non-negative and strictly less than p. Similarly, p divides the determinantal divisors of C_0 of size 2 given by

$$c_{i,j}c_{k,\ell} - c_{i,\ell}c_{k,j} = c_{i,j}c_{k,\ell} \tag{3.10}$$

for $1 \leqslant i < j < k < \ell \leqslant n$, such that $c_{i,j}c_{k,\ell} = 0$ too. ■

4. End of the proof of Theorem A

In this section, $n \geqslant 4$. The following lemma, whose proof can be skipped in a first reading, will be used in Proposition 4.2.

Lemma 4.1. *Let $n \geqslant 4$ and $2 \leqslant k \leqslant n-2$. Let $C = [c_{i,j}]_{1\leqslant i,j\leqslant n}$ be an upper-triangular matrix with integer entries satisfying*

$$\forall i \in \{1, \ldots, n\}, \quad c_{i,i} = p \tag{4.1}$$

and

$$1 \leqslant i < j \leqslant k < \ell \leqslant n \Rightarrow c_{i,j}c_{k,\ell} = 0 \tag{4.2}$$

for all positive integer i, j, k, ℓ. *Let*

$$2 \leqslant i_0 < j_0 \leqslant n-1. \tag{4.3}$$

Then, there exists ω_{i_0,j_0}, τ_{i_0,j_0} *in* $I_{n,k}$ *and* $\varepsilon_{i_0,j_0} = \pm 1$ *such that*

$$\left(CD^{(n)}(p)\right)(\omega_{i_0,j_0}, \tau_{i_0,j_0}) = \varepsilon_{i_0,j_0} p^{2k-2} c_{i_0,j_0}. \tag{4.4}$$

Proof of Lemma 4.1. Let $a_2 < a_3 < \cdots < a_{k-1}$ be an ordered sequence of indices in $\{2, \ldots, n-1\}$ not containing i_0 and j_0 and let

$$\begin{aligned} \omega_0 &= \{1, a_2, \ldots, a_{k-1}, a_k := i_0\}, \\ \tau_0 &= \{1, a_2, \ldots, a_{k-1}, j_0\}. \end{aligned}$$

Such a choice is possible by (4.3). Note that ω_0 and τ_0 do not belong a priori to $I_{n,k}$ since they are not necessarily ordered (see (2.11)) but on the one hand, this will only change the determinant occuring in the left-hand side of (4.4) by ± 1 and on the other hand, this abuse of notations has the advantage of minimizing a lot the notations involved.

By the Cauchy-Binet formula,

$$\begin{aligned} \left(CD^{(n)}(p)\right)(\omega_0, \tau_0) &= \sum_{\alpha \in I_{n,k}} C_0(\omega, \alpha) D^{(n)}(p)(\alpha, \tau) && (4.5) \\ &= C_0(\omega, \tau) D^{(n)}(p)(\tau, \tau) && (4.6) \\ &= p^{k-1} C_0(\omega, \tau) && (4.7) \\ &= p^k \sum_{\sigma \in \sigma_{k-1}} \varepsilon(\sigma) c_{a_{\sigma(2)},a_2} \ldots c_{a_{\sigma(k-1)},a_{k-1}} c_{a_{\sigma(k)},j_0} && (4.8) \end{aligned}$$

where σ_{k-1} stands for the group of permutations of $\{2, \ldots, k\}$.

Obviously, the contribution to the previous sum of the permutation Id in σ_{k-1} equals

$$p^{2k-2} c_{i_0,j_0}$$

by (4.1). This is exactly the right-hand side of (4.4), up to the abuse of notations recalled above.

Let us show that all the other terms vanish. Let $\sigma \neq \mathrm{Id}$ in σ_{k-1}. One can assume that $a_{\sigma(k)} \leqslant j_0$ and

$$a_{\sigma(\ell)} \leqslant a_\ell \tag{4.9}$$

for $\ell \in \{2, \ldots, k-1\}$ since otherwise, the contribution of σ trivially vanishes, C being upper-triangular. Let us say that

$$\begin{aligned} 2 \leqslant a_2 < \cdots < a_{u_0-1} < a_k = i_0 < a_{u_0} \\ < \cdots < a_{v_0} < j_0 < a_{v_0+1} < \cdots < a_{k-1} \leqslant n-1 \end{aligned} \tag{4.10}$$

where $2 \leqslant u_0 - 1 < v_0 \leqslant k-1$. (4.9) immediately implies that

$$\sigma(\ell) = \ell$$

for $2 \leqslant \ell \leqslant u_0 - 1$.

The fact that σ is different from the identity permutation Id entails that there exists at least two integers $\ell \geqslant u_0$ satisfying $\sigma(\ell) \neq \ell$. Let $u_0 \leqslant \ell_0 < \ell_1$ be the two consecutive smallest of them. One has

$$\sigma(\ell) = \ell$$

if $u_0 \leqslant \ell \leqslant \ell_0 - 1$ or $\ell_0 + 1 \leqslant \ell \leqslant \ell_1 - 1$ by (4.9), hence

$$\sigma(\ell_0) = k \qquad \text{and} \qquad \sigma(\ell_1) = \ell_0$$

by (4.10). Consequently, the contribution of σ equals

$$p^k \varepsilon(\sigma) c_{i_0, a_{\ell_0}} c_{a_{\ell_0}, a_{\ell_1}} \times \cdots = 0$$

by (4.2) since

$$1 \leqslant i_0 < a_{\ell_0} \leqslant a_{\ell_0} < a_{\ell_1}.$$

∎

Then, we need the following intermediate result.

Proposition 4.2. *Let $n \geqslant 4$. Let $C_0 = [c_{i,j}]_{1 \leqslant i,j \leqslant n}$ in $R_0^{(n)}(p)$. If*

$$\forall (i,j) \in \{1, \ldots, n\}^2, \quad 2 \leqslant i < j \leqslant n-1 \Rightarrow c_{i,j} = 0 \tag{4.11}$$

then

$$C_0 D^{(n)}(p) \in \Lambda_n \, diag\left(p, \underbrace{p^2, \ldots, p^2}_{n-2 \ terms}, p^3\right) \Lambda_n.$$

Otherwise,

$$C_0 D^{(n)}(p) \in \Lambda_n \, diag\left(p, p, \underbrace{p^2, \ldots, p^2}_{n-4 \ terms}, p^3, p^3\right) \Lambda_n.$$

In addition,

$$card\left(\left\{C_0 \in R_0^{(n)}(p), C_0 D^{(n)}(p) \in \Lambda_n \, diag\left(p, \underbrace{p^2, \ldots, p^2}_{n-2 \ terms}, p^3\right) \Lambda_n\right\}\right) = 2p^{n-1} - p - 1$$

and

$$card\left(\left\{C_0 \in R_0^{(n)}(p), C_0 D^{(n)}(p) \in \Lambda_n \, diag\left(p, p, \underbrace{p^2, \ldots, p^2}_{n-4 \ terms}, p^3, p^3\right) \Lambda_n\right\}\right) = \frac{p^2\left((n-3)p^{n-2} - (n-2)p^{n-3} + 1\right)}{p-1}.$$

Remark 4.3. One can easily check that when $n=3$

$$C_0 D^{(3)}(p) \in \Lambda_3 \mathrm{diag}\left(p, p^2, p^3\right) \Lambda_3$$

for all matrix $C_0 \in R_0^{(3)}(p)$ whereas when $n=2$

$$C_0 D^{(2)}(p) \in \Lambda_2 \mathrm{diag}\left(p, p^3\right) \Lambda_2$$

for all matrix $C_0 \in R_0^{(2)}(p)$.

Proof of Proposition 4.2. Recall that

$$\boldsymbol{d}_n\left(\mathrm{diag}\left(p, \underbrace{p^2, \ldots, p^2}_{n-2 \text{ terms}}, p^3\right)\right) = \left(p, p^3, \ldots, \underbrace{p^{2k-1}}_{k\text{'th term}}, \ldots, p^{2n-5}, p^{2n-3}, p^{2n}\right),$$

$$\boldsymbol{d}_n\left(\mathrm{diag}\left(p, p, \underbrace{p^2, \ldots, p^2}_{n-4 \text{ terms}}, p^3, p^3\right)\right) = \left(p, p^2, \ldots, \underbrace{p^{2k-2}}_{k\text{'th term}}, \ldots, p^{2n-6}, p^{2n-3}, p^{2n}\right),$$

$$\boldsymbol{d}_n(C_0) = \boldsymbol{d}_n(p) = \left(1, p, \ldots, \underbrace{p^{\ell-1}}_{\ell\text{'th term}}, \ldots, p^{n-2}, p^n\right)$$

for $2 \leqslant k \leqslant n-2$ and $2 \leqslant \ell \leqslant n-1$.

Obviously, $d_1(C_0 D^{(n)}(p)) = p$ and $d_n(C_0 D^{(n)}(p)) = p^{2n}$.

Let us show that $d_{n-1}(C_0 D^{(n)}(p)) = p^{2n-3}$. Of course, p^{2n-3} is a determinantal minor of $C_0 D^{(n)}(p)$ of size $n-1$ such that it remains to show that the other determinantal minors of $C_0 D^{(n)}(p)$ of size $n-1$ are all divisible by p^{2n-3}. Let $\omega = \{1, \ldots, n\} \setminus \{i_0\}$ and $\tau = \{1, \ldots, n\} \setminus \{j_0\}$ two elements in $I_{n,n-1}$ (see (2.11) for the notations used). By the Cauchy-Binet formula,

$$\begin{aligned}\left(C_0 D^{(n)}(p)\right)(\omega, \tau) &= \sum_{\alpha \in I_{n,n-1}} C_0(\omega, \alpha)\, D^{(n)}(p)(\alpha, \tau) \\ &= C_0(\omega, \tau)\, D^{(n)}(p)(\tau, \tau)\end{aligned}$$

since $D^{(n)}(p)$ is a diagonal matrix. If $j_0 = 1$ then $C_0(\omega, \tau)$ is divisible by p^{n-2}, since $d_{n-1}(C_0) = p^{n-2}$, and $D^{(n)}(p)(\tau, \tau) = p^n$. If $2 \leqslant j_0 \leqslant n-1$ then $C_0(\omega, \tau)$ is divisible by p^{n-2} and $D^{(n)}(p)(\tau, \tau) = p^{n-1}$. The only remaining case is when $j_0 = n$. The minor obtained when erasing the i_0'th row and the n'th column of $C_0 D^{(n)}(p)$ has its last row equal to 0 but when $i_0 = n$, in which case

$$\left(C_0 D^{(n)}(p)\right)(\omega, \tau) = p^{2n-3}.$$

Let $2 \leqslant k \leqslant n-2$. Of course, p^{2k-1} is a determinantal minor of $C_0 D^{(n)}(p)$ of size k. Then, by Lemma 4.1, all the integers

$$p^{2k-2} c_{i,j}$$

for $2 \leqslant i < j \leqslant n-1$ also belong to the list of determinantal minors of $C_0 D^{(n)}(p)$ of size k. Let $\omega = \{i_1, \ldots, i_k\}$ with $1 \leqslant i_1 < \cdots < i_k \leqslant n$ and $\tau = \{j_1, \ldots, j_k\}$ with $1 \leqslant j_1 < \cdots < j_k \leqslant n$ two elements in $I_{n,k}$. Once again, by the Cauchy-Binet formula,

$$\begin{aligned}\left(C_0 D^{(n)}(p)\right)(\omega, \tau) &= \sum_{\alpha \in I_{n,k}} C_0(\omega, \alpha) D^{(n)}(p)(\alpha, \tau) \\ &= C_0(\omega, \tau) D^{(n)}(p)(\tau, \tau) \\ &= C_0(\omega, \tau) \times \begin{cases} p^{k+1} & \text{if } 2 \leqslant j_1 < \cdots < j_{k-1} < j_k = n, \\ p^k & \text{if } 2 \leqslant j_1 < \cdots < j_k \leqslant n-1, \\ p^k & \text{if } 1 = j_1 < j_2 \cdots < j_{k-1} < j_k = n, \\ p^{k-1} & \text{if } 1 = j_1 < j_2 \cdots < j_k \leqslant n-1. \end{cases}\end{aligned}$$

$C_0(\omega, \tau)$ being divisible by p^{k-1}, since $d_k(C_0) = p^{k-1}$, all these determinantal minors are divisible by p^{2k-1} except a priori when $1 = j_1 < j_2 \cdots < j_k \leqslant n-1$. Let us investigate this last case. First of all,

$$\begin{aligned} C_0(\omega, \tau) &= \sum_{\sigma \in \sigma_k} \varepsilon(\sigma) c_{i_{\sigma(1)},1} c_{i_{\sigma(2)},j_2} \ldots c_{i_{\sigma(k)},j_k} \\ &= \sum_{\substack{\sigma \in \sigma_k \\ i_{\sigma(1)}=1}} \varepsilon(\sigma) c_{i_{\sigma(1)},1} c_{i_{\sigma(2)},j_2} \ldots c_{i_{\sigma(k)},j_k} \\ &= \begin{cases} p \sum_{\substack{\sigma \in \sigma_k \\ \sigma(1)=1}} \varepsilon(\sigma) c_{i_{\sigma(2)},j_2} \ldots c_{i_{\sigma(k)},j_k} & \text{if } i_1 = 1, \\ 0 & \text{otherwise} \end{cases} \end{aligned}$$

where σ_k stands for the permutation group on k letters and since the condition $i_{\sigma(1)} = 1$ is equivalent to $i_1 = \sigma(1) = 1$. We can focus on the case $i_1 = 1$, in which case

$$C_0(\omega, \tau) = \sum_{L=0}^{k-1} p^{1+L} \sum_{\substack{\sigma \in \sigma_k \\ \sigma(1)=1 \\ \forall \ell \in \{2,\ldots,k\}, i_{\sigma(\ell)} \leqslant j_\ell \\ \operatorname{card}\left(\left\{\ell \in \{2,\ldots,k\}, i_{\sigma(l)} = j_\ell\right\}\right) = L}} \varepsilon(\sigma) \prod_{\substack{2 \leqslant \ell \leqslant k \\ i_{\sigma(\ell)} \neq j_\ell}} c_{i_{\sigma(\ell)},j_\ell}$$

is a polynomial in a subset of

$$c_{i,j}, \quad 2 \leqslant i < j \leqslant n-1$$

divisible by p^{k-1}, since $d_k(C_0) = p^{k-1}$, whose constant term is divisible by p^k. One can now conclude as follows. If (4.11) holds then $d_k\left(C_0 D^{(n)}(p)\right)$ is the greatest common divisor of 0, p^{2k-1} and of a finite list of integers divisible by p^{2k-1}, hence

$$d_k\left(C_0 D^{(n)}(p)\right) = p^{2k-1}.$$

If (4.11) does not hold then $d_k\left(C_0 D^{(n)}(p)\right)$ is the greatest common divisors of p^{2k-1}, of the integers $p^{2k-2}c_{i,j}$, $2 \leqslant i < j \leqslant n-1$, and of a finite list of integers divisible by p^{2k-2}, hence

$$d_k\left(C_0 D^{(n)}(p)\right) = p^{2k-2}.$$

Let us compute the first cardinality, say $c_0^{(n)}(p)$, given in the previous proposition. The set

$$\left\{C_0 \in R_0^{(n)}(p), \forall (i,j) \in \{1,\ldots,n\}^2, \quad 2 \leqslant i < j \leqslant n-1 \Rightarrow c_{i,j} = 0\right\}$$

can be decomposed into the disjoint union of the three following sets.

- The set of matrices C_0 in $R_0^{(n)}(p)$ satisfying (4.11) and $c_{1,2} \neq 0$, $c_{n-1,n} = 0$, which implies that
$$c_{2,n} = \cdots = c_{n-2,n} = 0.$$
There are $(p-1)p^{n-2}$ such matrices.
- The set of matrices C_0 in $R_0^{(n)}(p)$ satisfying (4.11) and $c_{1,2} = 0$, $c_{n-1,n} \neq 0$, which implies that
$$c_{1,3} = \cdots = c_{1,n-1} = 0.$$
There are $(p-1)p^{n-2}$ such matrices.
- The set of matrices C_0 in $R_0^{(n)}(p)$ satisfying (4.11) and $c_{1,2} = c_{n-1,n} = 0$, which can be identified to the set of matrices C_0 in $R_0^{(n-1)}(p)$ satisfying (4.11), by erasing the diagonal of zeros above the main diagonal. There are $c_0^{(n-1)}(p)$ such matrices.

In total,

$$c_0^{(n)}(p) = 2(p-1)p^{n-2} + c_0^{(n-1)}(p).$$

One can conclude by induction on $n \geqslant 4$. If the formula holds for $n \geqslant 4$ then

$$c_0^{(n+1)}(p) = 2(p-1)p^{n-1} + 2p^{n-1} - p - 1 = 2p^n - p - 1.$$

Let us briefly check that $c_0^{(4)}(p) = 2p^3 - p - 1$. If C_0 in $R_0^{(4)}(p)$ satisfies (4.11) then five cases can occur.

- $c_{1,2} = c_{1,3} = c_{1,4} = c_{2,4} = 0$ and $c_{3,4} \neq 0$. There are $p-1$ such matrices.
- $c_{1,2} = c_{1,3} = c_{1,4} = 0$ and $c_{2,4} \neq 0$. There are $p(p-1)$ such matrices.
- $c_{1,2} = c_{1,3} = 0$ and $c_{1,4} \neq 0$. There are $p^2(p-1)$ such matrices.
- $c_{1,2} = c_{2,4} = c_{3,4} = 0$ and $c_{1,3} \neq 0$. There are $p(p-1)$ such matrices.
- $c_{2,4} = c_{3,4} = 0$ and $c_{1,2} \neq 0$. There are $p^2(p-1)$ such matrices.

The computation of the second cardinality is a consequence of Proposition 3.1, which gives the cardinal of $R_0^{(n)}(p)$. ■

Let us now complete the proof of Theorem A.

Proof of Theorem A. By (2.5),

$$\pi^{(n)}(p) * \pi^{(n)}(p) = \sum_{\Lambda_n h \Lambda_n \subset \pi^{(n)}(p)\pi^{(n)}(p)} m_n(h;p)\Lambda_n h \Lambda_n$$

where $h \in GL_n(\mathbb{Q})$ ranges over a system of representatives of the Λ_n right cosets contained in the set

$$\pi^{(n)}(p)\pi^{(n)}(p)$$

and

$$\begin{aligned} m_n(h;p) &\coloneqq \frac{\deg\left(D^{(n)}(p)\right)}{\deg(h)} c_n(h;p), \\ c_n(h;p) &\coloneqq \operatorname{card}\left(\left\{C \in R^{(n)}(p), CD^{(n)}(p) \in \pi^{(n)}(p)\right\}\right). \end{aligned}$$

Recall that

$$\deg\left(D^{(n)}(p)\right) = p\frac{\varphi_n(p)}{\varphi_1(p)^2\varphi_{n-2}(p)} = p\frac{\left(p^{n-1}-1\right)(p^n-1)}{(p-1)^2} \tag{4.12}$$

by (2.3).

Let us determine the different matrices h occuring in this decomposition.

If C_1 in $R_1^{(n)}(p)$ then we have already seen that

$$C_1 = \operatorname{diag}\left(p^{\delta_1}, \ldots, p^{\delta_n}\right) C_1'$$

with C_1' an upper-triangular matrix in Λ_n and $0 \leqslant \delta_1, \ldots, \delta_n \leqslant 2$ with

$$\operatorname{card}\left(\{i \in \{1,\ldots,n\}, \delta_i = 0\}\right) = \operatorname{card}\left(\{i \in \{1,\ldots,n\}, \delta_i = 2\}\right) = 1.$$

As a consequence,

$$\begin{aligned} C_1 D^{(n)}(p) &= \operatorname{diag}\left(p^{\delta_1}, \underbrace{p^{1+\delta_2}, \ldots, p^{1+\delta_{n-1}}}_{n-2 \text{ terms}}, p^{2+\delta_n}\right) D^{(n)}(p)^{-1} C_1' D^{(n)}(p) \\ &\in \Lambda_n \operatorname{diag}\left(p^{\delta_1}, \underbrace{p^{1+\delta_2}, \ldots, p^{1+\delta_{n-1}}}_{n-2 \text{ terms}}, p^{2+\delta_n}\right) \Lambda_n \end{aligned}$$

since $D^{(n)}(p)^{-1}C_1'D^{(n)}(p)$ belongs to Λ_n. Let $1 \leqslant \alpha_1 \neq \alpha_2 \leqslant n$ the integers satisfying

$$\delta_{\alpha_1} = 0 \qquad \text{and} \qquad \delta_{\alpha_2} = 2.$$

Let us list the different cases that can occur.

First case: $\alpha_1 = 1$ and $2 \leqslant \alpha_2 \leqslant n-1$. In this case, one has

$$C_1 D^{(n)}(p) \in \Lambda_n \mathrm{diag}\left(1, \underbrace{p^2, \ldots, p^2}_{n-3 \text{ terms}}, p^3, p^3\right) \Lambda_n.$$

The number of such matrices C_1 is

$$\sum_{2 \leqslant \alpha_2 \leqslant n-1} p^{n+\alpha_2-2} = p^n \frac{p^{n-2}-1}{p-1}. \tag{4.13}$$

Second case: $\alpha_1 = 1$ and $\alpha_2 = n$. In this case, one has

$$C_1 D^{(n)}(p) \in \Lambda_n \mathrm{diag}\left(1, \underbrace{p^2, \ldots, p^2}_{n-2 \text{ terms}}, p^4\right) \Lambda_n.$$

The number of such matrices C_1 is

$$p^{2n-2}. \tag{4.14}$$

Third case: $2 \leqslant \alpha_1 \leqslant n-1$ and $\alpha_2 = 1$. In this case, one has

$$C_1 D^{(n)}(p) \in \Lambda_n \mathrm{diag}\left(p, \underbrace{p^2, \ldots, p^2}_{n-2 \text{ terms}}, p^3\right) \Lambda_n.$$

The number of such matrices C_1 is

$$\sum_{2 \leqslant \alpha_1 \leqslant n-1} p^{n-\alpha_1} = p \frac{p^{n-2}-1}{p-1}. \tag{4.15}$$

Fourth case:[5] $2 \leqslant \alpha_1 \neq \alpha_2 \leqslant n-1$. In this case, one has

$$C_1 D^{(n)}(p) \in \Lambda_n \mathrm{diag}\left(p, p, \underbrace{p^2, \ldots, p^2}_{n-4 \text{ terms}}, p^3, p^3\right) \Lambda_n.$$

The number of such matrices C_1 is

$$\begin{aligned}\sum_{2 \leqslant \alpha_1 \neq \alpha_2 \leqslant n-1} p^{n-1+\alpha_2-\alpha_1} &= \left(\sum_{1 \leqslant \alpha \leqslant n-2} p^\alpha\right)^2 - (n-2)p^{n-1} \\ &= \frac{p^2\left(p^{2(n-2)} - (n-2)p^{n-1} + 2(n-3)p^{n-2} - (n-2)p^{n-3} + 1\right)}{(p-1)^2}. \end{aligned} \tag{4.16}$$

[5] Note that this case does not occur if $n < 4$.

Fifth case: $2 \leqslant \alpha_1 \leqslant n-1$ and $\alpha_2 = n$. In this case, one has

$$C_1 D^{(n)}(p) \in \Lambda_n \mathrm{diag}\left(p, p, \underbrace{p^2, \ldots, p^2}_{n-3 \text{ terms}}, p^4\right) \Lambda_n.$$

The number of such matrices C_1 is

$$\sum_{2 \leqslant \alpha_1 \leqslant n-1} p^{2n-1-\alpha_1} = p^n \frac{p^{n-2}-1}{p-1}. \tag{4.17}$$

Sixth case: $\alpha_1 = n$ and $\alpha_2 = 1$. In this case, one has

$$C_1 D^{(n)}(p) \in \Lambda_n \mathrm{diag}\left(\underbrace{p^2, \ldots, p^2}_{n \text{ terms}}\right) \Lambda_n = \Lambda_n p^2 I_n \Lambda_n.$$

The number of such matrices C_1 is

$$1. \tag{4.18}$$

Seventh case: $\alpha_1 = n$ and $2 \leqslant \alpha_2 \leqslant n-1$. In this case, one has

$$C_1 D^{(n)}(p) \in \Lambda_n \mathrm{diag}\left(p, \underbrace{p^2, \ldots, p^2}_{n-2 \text{ terms}}, p^3\right) \Lambda_n.$$

The number of such matrices C_1 is

$$\sum_{2 \leqslant \alpha_2 \leqslant n-1} p^{\alpha_2 - 1} = p \frac{p^{n-2}-1}{p-1}. \tag{4.19}$$

If C_0 in $R_0^{(n)}(p)$ then two cases can occur by Proposition 4.2.
Eighth case: $\forall (i,j) \in \{1, \ldots, n\}^2, 2 \leqslant i < j \leqslant n \Rightarrow c_{i,j} = 0$. In this case,

$$C_0 D^{(n)}(p) \in \Lambda_n \mathrm{diag}\left(p, \underbrace{p^2, \ldots, p^2}_{n-2 \text{ terms}}, p^3\right) \Lambda_n$$

and the number of such matrices is

$$2p^{n-1} - p - 1. \tag{4.20}$$

Nineth case: $\exists (i,j) \in \{1, \ldots, n\}^2, 2 \leqslant i < j \leqslant n$ and $c_{i,j} \neq 0$. In this case,

$$C_0 D^{(n)}(p) \in \Lambda_n \mathrm{diag}\left(p, p, \underbrace{p^2, \ldots, p^2}_{n-4 \text{ terms}}, p^3, p^3\right) \Lambda_n$$

and the number of such matrices is

$$\frac{p^2\left((n-3)p^{n-2}-(n-2)p^{n-3}+1\right)}{p-1}. \tag{4.21}$$

In particular, we have just proved that

$$\begin{aligned}
\pi^{(n)}(p)*\pi^{(n)}(p) = {} & m_n(1;p)\Lambda_n p^2 I_n \Lambda_n \\
& + m_n(2;p)\Lambda_n \mathrm{diag}\left(p, \underbrace{p^2,\dots,p^2}_{n-2 \text{ terms}}, p^3\right)\Lambda_n \\
& + m_n(3;p)\Lambda_n \mathrm{diag}\left(1, \underbrace{p^2,\dots,p^2}_{n-3 \text{ terms}}, p^3, p^3\right)\Lambda_n \\
& + m_n(4;p)\Lambda_n \mathrm{diag}\left(1, \underbrace{p^2,\dots,p^2}_{n-2 \text{ terms}}, p^4\right)\Lambda_n \\
& + m_n(5;p)\Lambda_n \mathrm{diag}\left(p, p, \underbrace{p^2,\dots,p^2}_{n-3 \text{ terms}}, p^4\right)\Lambda_n \\
& + m_n(6;p)\Lambda_n \mathrm{diag}\left(p, p, \underbrace{p^2,\dots,p^2}_{n-4 \text{ terms}}, p^3, p^3\right)\Lambda_n .
\end{aligned} \tag{4.22}$$

where

$$\begin{aligned}
m_n(1;p) &\coloneqq m_n\left(p^2 I_n; p\right), \\
m_n(2;p) &\coloneqq m_n\left(\mathrm{diag}\left(p, \underbrace{p^2,\dots,p^2}_{n-2 \text{ terms}}, p^3\right); p\right), \\
m_n(3;p) &\coloneqq m_n\left(\mathrm{diag}\left(1, \underbrace{p^2,\dots,p^2}_{n-3 \text{ terms}}, p^3, p^3\right); p\right)
\end{aligned}$$

and

$$\begin{aligned}
m_n(4;p) &\coloneqq m_n\left(\mathrm{diag}\left(1, \underbrace{p^2,\dots,p^2}_{n-2 \text{ terms}}, p^4\right); p\right), \\
m_n(5;p) &\coloneqq m_n\left(\mathrm{diag}\left(p, p, \underbrace{p^2,\dots,p^2}_{n-3 \text{ terms}}, p^4\right); p\right), \\
m_n(6;p) &\coloneqq m_n\left(\mathrm{diag}\left(p, p, \underbrace{p^2,\dots,p^2}_{n-4 \text{ terms}}, p^3, p^3\right); p\right).
\end{aligned}$$

One has,

$$m_n(1;p) = \frac{\deg\left(D^{(n)}(p)\right)}{\deg(p^2 I_n)} c_n\left(p^2 I_n; p\right) = p\frac{\left(p^{n-1}-1\right)\left(p^n-1\right)}{(p-1)^2}$$

by (4.12) and (4.18) since $\deg(p^2 I_n) = 1$.

Then,

$$\begin{aligned}
m_n(2;p) &= \frac{\deg\left(D^{(n)}(p)\right)}{\deg\left(\mathrm{diag}\left(p, \underbrace{p^2,\ldots,p^2}_{n-2 \text{ terms}}, p^3\right)\right)} c_n\left(\mathrm{diag}\left(p, \underbrace{p^2,\ldots,p^2}_{n-2 \text{ terms}}, p^3\right); p\right) \\
&= c_n\left(\mathrm{diag}\left(p, \underbrace{p^2,\ldots,p^2}_{n-2 \text{ terms}}, p^3\right); p\right) \\
&= 2p\frac{p^{n-2}-1}{p-1} + 2p^{n-1} - p - 1 \\
&= \frac{2p^n - p^2 - 2p + 1}{p-1}
\end{aligned}$$

by (2.2), (4.15), (4.19), (4.20).

Let us compute simultaneously the values of $m_n(3;p)$ and $m_n(4;p)$. On the one hand, applying the map Ψ (see (2.14)) to (4.22), one gets

$$\begin{aligned}
\pi^{(n-1)}_{n-2,1}(p) * \pi^{(n-1)}_{n-2,1}(p) = {} & m_n(3;p)\Lambda_n \mathrm{diag}\left(\underbrace{p^2,\ldots,p^2}_{n-3 \text{ terms}}, p^3, p^3\right)\Lambda_n \\
&+ m_n(4;p)\Lambda_n \mathrm{diag}\left(\underbrace{p^2,\ldots,p^2}_{n-2 \text{ terms}}, p^4\right)\Lambda_n.
\end{aligned}$$

On the other hand, by [AZ95, Lemma 2.18 Equation (2.30), p. 115], one gets

$$\begin{aligned}
\pi^{(n-1)}_{n-2,1}(p) * \pi^{(n-1)}_{n-2,1}(p) &= \Lambda_n p^2 I_n \Lambda_n * \pi^{(n-1)}_{1}(p) * \pi^{(n-1)}_{1}(p) \\
&= \Lambda_n p^2 I_n \Lambda_n * \left(\pi^{(n-1)}_{0,1}(p) + (p+1)\pi^{(n-1)}_{2,0}(p)\right) \\
&= \Lambda_n \mathrm{diag}\left(\underbrace{p^2,\ldots,p^2}_{n-2 \text{ terms}}, p^4\right)\Lambda_n \\
&\quad + (p+1)\Lambda_n \mathrm{diag}\left(\underbrace{p^2,\ldots,p^2}_{n-3 \text{ terms}}, p^3, p^3\right)\Lambda_n
\end{aligned}$$

by (2.9). Distinct Λ_n double cosets being linearly independent by [AZ95, Lemma 1.5, p. 96], we get

$$m_n(3;p) = p+1, \qquad m_n(4;p) = 1.$$

Then,

$$\begin{aligned}\deg\left(\operatorname{diag}\left(1,\underbrace{p^2,\ldots,p^2}_{n-3\text{ terms}},p^3,p^3\right)\right)&\\ &= \frac{\deg\left(D^{(n)}(p)\right)}{m_n(3;p)} c_n\left(\operatorname{diag}\left(1,\underbrace{p^2,\ldots,p^2}_{n-3\text{ terms}},p^3,p^3\right);p\right)\\ &= p^{n+1}\frac{\left(p^{n-2}-1\right)\left(p^{n-1}-1\right)\left(p^n-1\right)}{(p-1)^2\left(p^2-1\right)}\end{aligned}$$

by (4.12) and (4.13). This proves (1.8) in Theorem A. Similarly,

$$\begin{aligned}\deg\left(\operatorname{diag}\left(1,\underbrace{p^2,\ldots,p^2}_{n-2\text{ terms}},p^4\right)\right) &= \frac{\deg\left(D^{(n)}(p)\right)}{m_n(4;p)} c_n\left(\operatorname{diag}\left(1,\underbrace{p^2,\ldots,p^2}_{n-2\text{ terms}},p^4\right);p\right)\\ &= p^{2n-1}\frac{\left(p^{n-1}-1\right)\left(p^n-1\right)}{(p-1)^2}\end{aligned}$$

by (4.12) and (4.14). This proves (1.9) in Theorem A.

Let us consider $m_n(5;p)$. First, let us compute the value of

$$\deg\left(\operatorname{diag}\left(p,p,\underbrace{p^2,\ldots,p^2}_{n-3\text{ terms}},p^4\right)\right) = \deg\left(\operatorname{diag}\left(1,1,\underbrace{p,\ldots,p}_{n-3\text{ terms}},p^3\right)\right)$$

by (2.2). This is done by a semi-explicit computation of

$$\pi_{n-2}^{(n)}(p) * \pi_{0,1}^{(n)}(p) = \sum_{\Lambda_n h\Lambda_n\subset\pi_{n-2}^{(n)}(p)\pi_{0,1}^{(n)}(p)} m\left(D_{n-2}^{(n)}(p), D_{0,1}^{(n)}(p);h\right)\Lambda_n h\Lambda_n$$

where $h\in GL_n(\mathbb{Q})$ ranges over a system of representatives of the Λ_n right cosets contained in the set

$$\pi_{n-2}^{(n)}(p)\pi_{0,1}^{(n)}(p)$$

and

$$\begin{aligned}m\left(D_{n-2}^{(n)}(p), D_{0,1}^{(n)}(p);h\right)&\\ &= \frac{\deg\left(D_{0,1}^{(n)}(p)\right)}{\deg(h)}\operatorname{card}\left(\left\{C\in R_{1,1,\underbrace{p,\ldots,p}_{n-2}}, CD_{0,1}^{(n)}(p)\in\Lambda_n h\Lambda_n\right\}\right)\end{aligned}$$

where $R_{1,1,\underbrace{p,\ldots,p}_{n-2}}$ is the complete system of representatives for the distinct Λ_n right cosets of $\pi^{(n)}_{n-2}(p)$ modulo Λ_n given by the set of upper-triangular column reduced matrices C satisfying

$$\forall i\in\{1,\ldots,n\}\,,\quad c_{i,i}\in\{1,p\}, \tag{4.23}$$

$$\mathrm{card}\left(\{i\in\{1,\ldots,n\},c_{i,i}=1\}\right)=2 \tag{4.24}$$

and

$$\forall i\in\{1,\ldots,n-1\}\,,p\mid c_{i,i}\Rightarrow\forall j\in\{i+1,\ldots,n\}\,,\quad c_{i,j}=0 \tag{4.25}$$

according to [AZ95, Lemma 2.18, p. 115]. Let C be an element of $R_{1,1,\underbrace{p,\ldots,p}_{n-2}}$ and let $1\leqslant\alpha_1<\alpha_2\leqslant n$ be the indices of the diagonal elements of C equal to 1 by (4.24). By (4.23) and (4.25), C can be decomposed into

$$C=\mathrm{diag}\left(p^{\delta_1},\ldots,p^{\delta_n}\right)C'$$

for some upper-triangular matrix C' in Λ_n and integers $0\leqslant\delta_1,\ldots,\delta_n\leqslant 1$ such that

$$CD^{(n)}_{0,1}(p)\in\begin{cases}\Lambda_n\mathrm{diag}\left(1,1,\underbrace{p,\ldots,p}_{n-3\text{ terms}},p^3\right)\Lambda_n & \text{if } 1\leqslant\alpha_1<\alpha_2\leqslant n-1\\ \pi^{(n)}_{n-2,1}(p) & \text{if } 1\leqslant\alpha_1<\alpha_2=n.\end{cases}$$

Thus,

$$\begin{aligned}\pi^{(n)}_{n-2}(p)*\pi^{(n)}_{0,1}(p)&=m\left(D^{(n)}_{n-2}(p),D^{(n)}_{0,1}(p);D^{(n)}_{n-2,1}(p)\right)\pi^{(n)}_{n-2,1}(p)\\&\quad+m\left(D^{(n)}_{n-2}(p),D^{(n)}_{0,1}(p);\mathrm{diag}\left(1,1,\underbrace{p,\ldots,p}_{n-3\text{ terms}},p^3\right)\right)\\&\quad\times\Lambda_n\mathrm{diag}\left(1,1,\underbrace{p,\ldots,p}_{n-3\text{ terms}},p^3\right)\Lambda_n.\end{aligned}$$

Applying the map $\Psi^{\circ 2}$ (see (2.14)) to the previous equality, one gets

$$\begin{aligned}&\Lambda_n\mathrm{diag}\left(\underbrace{p,\ldots,p}_{n-3\text{ terms}},p^3\right)\Lambda_n\\&=m\left(D^{(n)}_{n-2}(p),D^{(n)}_{0,1}(p);\mathrm{diag}\left(\underbrace{p,\ldots,p}_{n-3\text{ terms}},p^3\right)\right)\Lambda_n\mathrm{diag}\left(\underbrace{p,\ldots,p}_{n-3\text{ terms}},p^3\right)\Lambda_n,\end{aligned}$$

hence

$$m\left(D^{(n)}_{n-2}(p), D^{(n)}_{0,1}(p); \mathrm{diag}\left(\underbrace{p,\ldots,p}_{n-3\text{ terms}}, p^3\right)\right) = 1$$

by the linear independence of distinct Λ_n double cosets ([AZ95, Lemma 1.5 Equation (2.32), p. 96]). As a consequence,

$$\begin{aligned}
\deg\left(\mathrm{diag}\left(1,1,\underbrace{p,\ldots,p}_{n-3\text{ terms}}, p^3\right)\right) &= \deg\left(D^{(n)}_{0,1}(p)\right) \sum_{1\leqslant\alpha_1<\alpha_2\leqslant n-1} p^{2n-1-\alpha_1-\alpha_2} \\
&= p^{n-1}\frac{\varphi_n(p)}{\varphi_{n-1}(p)\varphi_1(p)} p^{2n-1} \sum_{1\leqslant\alpha_1<\alpha_2\leqslant n-1} \left(\frac{1}{p}\right)^{\alpha_1+\alpha_2} \\
&= p^{n-1}\frac{\varphi_n(p)}{\varphi_{n-1}(p)\varphi_1(p)} p^{2n-4} \frac{\varphi_{n-1}(1/p)}{\varphi_2(1/p)\varphi_{n-3}(1/p)} \\
&= p^{n-1}\frac{\varphi_n(p)}{\varphi_{n-1}(p)\varphi_1(p)} p^{2} \frac{\varphi_{n-1}(p)}{\varphi_2(p)\varphi_{n-3}(p)} \\
&= p^{n+1}\frac{\varphi_n(p)}{\varphi_1(p)\varphi_2(p)\varphi_{n-3}(p)}
\end{aligned}$$

by (4.12), [AZ95, Equation (2.33), p. 115] and since

$$\varphi_r(1/x) = (-1)^r x^{-r(r+1)/2}\varphi_r(x)$$

for $r \geqslant 1$ and $x \neq 0$ a real number. This proves (1.10) in Theorem A. As a consequence,

$$\begin{aligned}
m_n(5;p) &= \frac{\deg\left(D^{(n)}(p)\right)}{\deg\left(\mathrm{diag}\left(p,p,\underbrace{p^2,\ldots,p^2}_{n-3\text{ terms}},p^4\right)\right)} c_n\left(\mathrm{diag}\left(p,p,\underbrace{p^2,\ldots,p^2}_{n-3\text{ terms}},p^4\right);p\right) \\
&= \frac{\varphi_2(p)}{\varphi_1(p)^2} \\
&= p+1
\end{aligned}$$

by (4.17).

Finally, let us compute the value of $m_n(6;p)$. One has

$$\begin{aligned} m_n(6;p) &= \frac{\deg\left(D^{(n)}(p)\right)}{\deg\left(\operatorname{diag}\left(p,p,\underbrace{p^2,\ldots,p^2}_{n-4\text{ terms}},p^3,p^3\right)\right)} \\ &\qquad \times c_n\left(\operatorname{diag}\left(p,p,\underbrace{p^2,\ldots,p^2}_{n-4\text{ terms}},p^3,p^3\right);p\right) \\ &= \frac{\deg\left(D^{(n)}(p)\right)}{\deg\left(D^{(n)}_{n-4,2}(p)\right)} c_n\left(\operatorname{diag}\left(p,p,\underbrace{p^2,\ldots,p^2}_{n-4\text{ terms}},p^3,p^3\right);p\right) \\ &= \frac{(p+1)^2(p-1)^2}{p^3\left(p^{n-2}-1\right)\left(p^{n-3}-1\right)} \frac{p^3\left(p^{2n-5}-p^{n-2}-p^{n-3}+1\right)}{(p-1)^2} \\ &= (p+1)^2 \end{aligned}$$

by (2.2), (2.3), (4.16) and (4.21).

Equation (4.22) and the explicit values of the constants $m_n(i;p)$ $(1 \leqslant i \leqslant 6)$ prove (1.12) in Theorem A. ■

References

[AZ95] A.N. Andrianov and V.G. Zhuravlëv, *Modular forms and Hecke operators*, volume 145 of Translations of Mathematical Monographs, American Mathematical Society, Providence, RI, 1995, Translated from the 1990 Russian original by Neal Koblitz.

[BB] V. Blomer and J. Buttcane, *On the subconvexity problem for L-functions on $GL(3)$*, available at http://arxiv.org/abs/1504.02667.

[BH10] V. Blomer and R. Holowinsky, *Bounding sup-norms of cusp forms of large level*, Invent. Math. **179**(3) (2010), 645–681.

[BHM] V. Blomer, G. Harcos, and D. Milicevic, *Eigenfunctions on arithmetic hyperbolic 3-manifolds*, Duke Math. J. **165**(4) (2016), 625–659.

[Blo12] V. Blomer, *Subconvexity for twisted L-functions on* GL(3), Amer. J. Math. **134**(5) (2012), 1385–1421.

[BMa] V. Blomer and P. Maga, *Subconvexity for sup-norms of automorphic forms on $PGL(n)$*, available at http://arxiv.org/pdf/1405.6691.pdf.

[BMb] V. Blomer and P. Maga, *The sup-norm problem for $PGL(4)$*, Int. Math. Res. Not. **14** (2015), 5311–5332.

[BT] F. Brumley and N. Templier, *Large values of cusp forms on $GL(n)$*, available at http://arxiv.org/abs/1411.4317.

[Bur62] D.A. Burgess, *On character sums and L-series*, Proc. London Math. Soc. (3) **12** (1962), 193–206.

[DFI94] W. Duke, J.B. Friedlander, and H.Iwaniec, *Bounds for automorphic L-functions. II*, Invent. Math. **115**(2) (1994), 219–239.

[FI92] J. Friedlander and H. Iwaniec, *A mean-value theorem for character sums*, Michigan Math. J. **39**(1) (1992), 153–159.

[Gol06] D. Goldfeld, *Automorphic forms and L-functions for the group $GL(n, \mathbb{R})$*, volume 99 of Cambridge Studies in Advanced Mathematics, Cambridge University Press, Cambridge, 2006 (with an appendix by Kevin A. Broughan).

[HR] H. Helfgott and G. Ricotta, *A new bound for the sup-norm of automorphic forms on non-compact modular curves in the level aspect*, available at http://www.math.u-bordeaux1.fr/gricotta/supnorm.htm.

[HRRa] R. Holowinsky, G. Ricotta, and E. Royer, *The amplification method in the $GL(3)$ Hecke algebra*, available at http://arxiv.org/abs/1412.5022.

[HRRb] R. Holowinsky, G. Ricotta, and E. Royer, *On the sup-norm of $SL(3)$ Hecke-Maass cusp form*, available at http://arxiv.org/abs/1411.4317.

[HT12] G. Harcos and N. Templier, *On the sup-norm of Maass cusp forms of large level: II*, Int. Math. Res. Not. IMRN **20** (2012), 4764–4774.

[HT13] G. Harcos and N. Templier, *On the sup-norm of Maass cusp forms of large level. III*, Math. Ann. **356**(1) (2013), 209–216.

[IS95] H. Iwaniec and P. Sarnak, *L^∞ norms of eigenfunctions of arithmetic surfaces*, Ann. of Math. (2) **141**(2) (1995), 301–320.

[Iwa92] H. Iwaniec, *The spectral growth of automorphic L-functions*, J. Reine Angew. Math. **428** (1992), 139–159.

[Kri90] A. Krieg, *Hecke algebras*, Mem. Amer. Math. Soc. **87**(435) (1990), x+158.

[Li11] X. Li, *Bounds for* $\mathrm{GL}(3) \times \mathrm{GL}(2)$ *L-functions and* $\mathrm{GL}(3)$ *L-functions*, Ann. of Math. (2) **173**(1) (2011), 301–336.

[Mara] S. Marshall, *Local bounds for L^p norms of Maass forms in the level aspect*, available at http://arxiv.org/abs/1502.01006.

[Marb] S. Marshall, *Sup norms of Maass forms on semisimple groups*, available at http://arxiv.org/abs/1405.7033.

[Muna] R. Munshi, *The circle method and bounds for L-functions - III: t-aspect subconvexity for $GL(3)$ L-functions*, . Amer. Math. Soc. **28**(4) (2015), 913–938.

[Munb] R. Munshi, *The circle method and bounds for L-functions - IV: subconvexity for twists of* $\mathrm{GL}(3)$ *L-functions*, Ann. of Math. (2) **182** (2015), 617–672.

[MV10] P. Michel and A. Venkatesh, *The subconvexity problem for* GL_2, Publ. Math. Inst. Hautes Études Sci. **111** (2010), 171–271.

[New72] M. Newman, *Integral matrices*, Academic Press, New York, 1972. Pure and Applied Mathematics, Vol. 45.

[Sah] A. Saha, *On sup-norms of cusp forms of powerful level*, available at http://arxiv.org/abs/1404.3179.

[Sar] P. Sarnak, *Letter to Morawetz*, available at http://www.math.princeton.edu/sarnak.

[Shi94] G. Shimura, *Introduction to the arithmetic theory of automorphic functions*, volume 11 of Publications of the Mathematical Society of Japan, Princeton University Press, Princeton, NJ, 1994. Reprint of the 1971 original, Kanô Memorial Lectures 1.

[SV] L. Silberman and A. Venkatesh, *Entropy bounds for Hecke eigenfunctions on division algebras*, preprint available at http://www.math.ubc.ca/lior/work/.

[Tem10] N. Templier, *On the sup-norm of Maass cusp forms of large level*, Selecta Math. (N.S.) **16**(3) (2010), 501–531.

[Wey21] H. Weyl, *Zur abschatzung von* $\zeta(1+ti)$, Math. Z. **10** (1921), 88–101.

Address: Guillaume Ricotta: Université de Bordeaux, Institut de Mathématiques de Bordeaux, 351 cours de la libération, 33405 Talence Cedex, France.

E-mail: Guillaume.Ricotta@math.u-bordeaux1.fr

Received: 16 March 2015; **revised:** 19 November 2015