

THE SUP-NORM PROBLEM FOR AUTOMORPHIC CUSP FORMS OF $\mathrm{PGL}(n, \mathbb{Z}[i])$

PÉTER MAGA AND GERGELY ZÁBRÁDI

ABSTRACT. Let ϕ be an L^2 -normalized Hecke–Maaß cusp form for $\mathrm{PGL}_n(\mathbb{Z}[i])$ on the locally symmetric space $X := \mathrm{PGL}_n(\mathbb{Z}[i]) \backslash \mathrm{PGL}_n(\mathbb{C}) / \mathrm{PU}_n$. If Ω is a compact subset of X , then we prove the bound $\|\phi|_{\Omega}\|_{\infty} \ll_{\Omega} \lambda_{\phi}^{n(n-1)/4-\delta}$ for some $\delta > 0$ depending only on n , where λ_{ϕ} is the Laplace eigenvalue of ϕ .

1. INTRODUCTION

Given a Riemannian locally symmetric space $X = \Gamma \backslash S$, it is a classical analytic problem to give pointwise bounds for (L^2 -normalized) eigenfunctions F of the algebra of invariant differential operators $\mathcal{D}(S)$, uniformly in S in terms of the Laplace eigenvalue λ_F of F . If X is compact, then Sarnak [Sar] proved the baseline bound

$$(1) \quad \|F\|_{\infty} \ll_X \lambda_F^{\frac{\dim(X) - \mathrm{rk}(X)}{4}}.$$

The exponent on the right-hand side is known to be sharp in general. It is also known in some special cases that if X is not compact, then $\|F\|_{\infty}$ might be considerably larger (see [BT20]), but (1) still holds if F is restricted to compact subsets of X . The sup-norm problem in the theory of automorphic forms asks if the exponent of (1) can be strengthened if X is an arithmetic manifold and F is an eigenfunction not only of $\mathcal{D}(S)$ but of the full Hecke algebra of X .

An important motivation comes from quantum mechanics. Classical mechanics interprets a freely moving particle as a geodesic flow. The quantum mechanical interpretation of the same object is an L^2 -normalized linear combination of eigenstates. Since the geodesic flow is ergodic with respect to the Liouville measure on the tangent space, the correspondence principle of quantum mechanics suggests that the masses of the eigenstates reproduce the invariant measure in the high-energy limit. Bounds on the sup-norm (or in general, the L^p norm for any $p > 2$) of eigenstates control their mass concentration, and hence are in connection with the quantum unique ergodicity conjecture of Rudnick and Sarnak [RS94]. Other important connections of sup-norm bounds are towards the multiplicity problem, nodal domains of automorphic forms and bounds for L -functions, see e.g. [Sar], [GRS13], [BH10].

In improving (1), there are (at least) two independent directions of research: one is to find as strong power-savings as possible among special circumstances, typically in rank one (see e.g. [IS95] and [BHMM20]), the other one is to find any power-saving in higher rank or among as general circumstances as possible (see e.g. [BP16], [BM15], [BM16]). We pick up the thread in the second theme, where the current limitation of our knowledge is an unpublished manuscript [Mar], which proves power-saving for a wide class of symmetric spaces, more specifically, for arithmetic quotients of quasi-split groups with the exception of the type $\mathrm{SU}(n, n-1)$. (We note that even though [Mar] is not peer-reviewed, it is widely accepted in the community as being correct.)

In these notes, we introduce a new method, based and improved on that of [BM16], to tackle the sup-norm problem. As a test application, we prove a saving over (1) in the case of the locally symmetric space

$$X := \Gamma \backslash G / K, \quad \Gamma := \mathrm{PGL}_n(\mathbb{Z}[i]), \quad G := \mathrm{PGL}_n(\mathbb{C}), \quad K := \mathrm{PU}_n.$$

Admittedly, our result follows from the main result of [Mar] (see especially [Mar, Corollary 1.4]), but we strongly believe that the novelty of the method deserves attention, and might have the potential to address the type $\mathrm{SU}(n, n-1)$, the exceptional case in Marshall’s work.

2020 *Mathematics Subject Classification*. 11F55, 11F72, 11D75.

Key words and phrases. automorphic forms in higher rank, sup-norm problem, Hecke operators, trace formula, diophantine approximation, amplification.

All along the paper, we think of $n \geq 2$ as being fixed, in particular, all implied constants below are allowed to depend on n .

Before stating our main result, we fix some notations. Since it is convenient to work with matrices instead of their projectivization, we shall realize elements of G as the rightmost nonzero entry of the bottom row is 1. We will also talk about points of X or G/K as matrices, by which we mean any matrix which represents them. Let A stand for the diagonal subgroup of G consisting of positive real entries and let N be the upper-triangular unipotent subgroup. Then the Iwasawa decomposition reads as $G = NAK$. We write \mathfrak{a} for the Lie algebra of A , \mathfrak{a}^* for its dual and $\mathfrak{a}_{\mathbb{C}}^*$ for the complexification of \mathfrak{a}^* . Fixing bases in \mathfrak{a}^* and $\mathfrak{a}_{\mathbb{C}}^*$, we may view them as appropriate subsets of \mathbb{R}^n and \mathbb{C}^n , respectively. Let W stand for the Weyl group, Σ for the set of roots and Σ^+ for the set of positive roots corresponding to N . For $\alpha \in \Sigma$, let $m(\alpha)$ be the real dimension of the corresponding root space. For $\lambda \in \mathfrak{a}^*$, define

$$D(\lambda) := \prod_{\alpha \in \Sigma^+} (1 + |\langle \alpha, \lambda \rangle|)^{m(\alpha)},$$

where $\langle \cdot, \cdot \rangle$ is induced by the Killing form.

In our special situation, define, for $1 \leq j \leq n$, the function e_j on \mathfrak{a} as $e_j(\text{diag}(a_1, \dots, a_n)) = a_j$, and then a set of positive roots is given by $e_j - e_k$ with $1 \leq j < k \leq n$. The corresponding root space is spanned by the matrices E_{jk} and iE_{jk} , where E_{jk} is the matrix which 1 at position j, k and otherwise zero, hence $m(e_j - e_k) = 2$.

A Hecke–Maaß cusp form ϕ on X comes with archimedean Langlands parameters $\mu_\phi = (\mu_1, \dots, \mu_n) \in \mathfrak{a}_{\mathbb{C}}^*/W \subset \mathbb{C}^n/W$ such that $\mu_1 + \dots + \mu_n = 0$ and $\{\mu_1, \dots, \mu_n\} = \{\overline{\mu_1}, \dots, \overline{\mu_n}\}$. In our parametrization, $(\mu_1, \dots, \mu_n) \in \mathbb{R}^n$ corresponds to the tempered spectrum, and we have that $\Im \mu_1, \dots, \Im \mu_n = O(1)$. Let μ_ϕ^* stand for $\Re \mu_\phi$. Since for the Laplace eigenvalue λ_ϕ of ϕ ,

$$\lambda_\phi \asymp 1 + \|\mu_1\|^2 + \dots + \|\mu_n\|^2$$

holds, we have

$$D(\mu_\phi^*) \ll \lambda_\phi^{\frac{n(n-1)}{2}}.$$

The main result of this paper is the following.

Theorem 1. *For any $n \geq 2$, there exists some $\delta = \delta(n) > 0$ with the following property. For any L^2 -normalized Hecke–Maaß cusp form ϕ on X and any compact $\Omega \subset X$,*

$$\|\phi|_\Omega\|_\infty \ll_\Omega D(\mu_\phi^*)^{\frac{1}{2}-\delta}.$$

In particular,

$$\|\phi|_\Omega\|_\infty \ll_\Omega \lambda_\phi^{\frac{n(n-1)}{4}(1-2\delta)}.$$

Since $n(n-1)/4 = (\dim(X) - \text{rk}(X))/4$, this is a saving over (1). We note that the case $n = 2$ was solved in [BHM16].

Our method closely follows the one introduced in [BM16], however, the counting problem in this situation is more challenging (because of the too large maximal compact subgroup of G , as it will be briefly exposed below). This requires an improvement in the counting techniques, which is the heart of this paper (vaguely speaking, a combination of Lemma 4 and Lemma 8). As a by-product, there is no need of Linnik type theorems about small primes in arithmetic progressions (i.e. zero repulsion of L -functions) any more.

We remark that with some work, the jungle of $O(1)$'s below (particularly in Section 4) can be made explicit, hence an explicit subconvexity saving is available, see the work [Gil20] over the rational field (in fact, now it is easier, since the reference to Linnik type theorems is removed). We also note that the implied constant (which depends on Ω) can be also made fully explicit, so the method in principle is effective, e.g. we do not need any reference to Siegel zeroes.

Acknowledgements. We thank Valentin Blomer for useful discussions about the topic of the paper. We also thank Gergely Harcos and Vitezslav Kala for discussions about some closely related questions.

The research towards this work was supported by NKFIH (National Research, Development and Innovation Office) Grants KKP 133819 (PM), FK 135218 (PM), FK 127906 (GZ), K 135885 (GZ), ELKH (Eötvös Loránd Research Network) Grant SA-71/2021 (PM & GZ), and the MTA Rényi Intézet Lendület Automorphic Research Group (PM & GZ).

2. REDUCTION TO A COUNTING PROBLEM

In this section, we reduce the problem to a matrix counting problem, following the lines of [BM15] and [BM16], where $\mathrm{PGL}_n(\mathbb{Z}) \backslash \mathrm{PGL}_n(\mathbb{R}) / \mathrm{PO}_n$ was treated. Since the spherical Hecke algebra is isomorphic in that case to ours at the archimedean and all relevant non-archimedean places, almost everything follows verbatim, so we give only a brief exposition, with some emphasis on the small difference coming from the fact that the maximal compact subgroup is the orthogonal group in the real case and the unitary group in the complex case.

Let $f_{\mu_\phi} : K \backslash G / K \rightarrow \mathbb{C}$ be the spherical function constructed in [BM16, pp.1276–1277] (here we utilize that $A, \mathfrak{a}^*, \mathfrak{a}_\mathbb{C}^*$ are the same for $\mathrm{PGL}_n(\mathbb{R})$ and $\mathrm{PGL}_n(\mathbb{C})$). Denoting by \tilde{f}_{μ_ϕ} its spherical transform, for any $x, y \in G$, we have the pre-trace formula

$$(2) \quad \int \tilde{f}_{\mu_\phi}(\mu_\varpi) \overline{F_\varpi(x)} F_\varpi(y) d\varpi = \sum_{\gamma \in \Gamma} f_{\mu_\phi}(x^{-1}\gamma y),$$

where the integral on the left is meant over the full spectrum of $\Gamma \backslash G$.

The idea of amplification in the current setup can be summarized as follows. Assume we want to estimate our form ϕ at a point $g \in \Omega$. Then in (2), we set $x := g$ and we take y of the form γg , where γ runs through right coset representatives corresponding to certain Hecke operators. An appropriate weighted sum of these results in a positive operator on $L^2(X)$, hence from the left-hand side, all but the one term corresponding to $F_\varpi = \phi$ can be dropped (for this positivity argument, see also [BHMM20, Section 3]). All in all, we arrive at a bound of the form

$$C|\phi(g)|^2 \leq \sum_{\gamma \in \Gamma'} f_{\mu_\phi}(g^{-1}\gamma g)$$

with Γ' being a finite set of matrices arising from the Hecke operators utilized, and C is a positive constant coming from \tilde{f}_{μ_ϕ} and the corresponding Hecke eigenvalues. Then, using that f_{μ_ϕ} decays controllably away from K (see [BP16, Theorem 2]), to bound $|\phi(g)|$, we essentially have to count those $\gamma \in \Gamma'$ for which $g^{-1}\gamma g$ is close to K .

To be a little more concrete, let $L \geq 2$ be a parameter, and assume that \mathcal{P} is a set of primes π lying above distinct split rational primes such that $L \leq N(\pi) < 2L$ with N standing for the norm. Then the discussion of [BM15, Sections 4, 6] (which in fact uses [BP16, Theorem 2], and see also [BM16, Section 2]) leads to, for any number $M \geq 1$,

$$(3) \quad |\phi(g)|^2 \ll_{M, \Omega} D(\mu_\phi^*) \cdot \left(\frac{1}{\#\mathcal{P}} + D(\mu_\phi^*)^{-\kappa} L^K + \sum_{\nu=1}^n \frac{1}{(\#\mathcal{P})^2} \sum_{\pi, \pi' \in \mathcal{P}} \frac{\#S(Q, \pi^\nu, \pi'^\nu, M)}{L^{\nu(n-1)}} \right), \quad g \in \Omega,$$

where K is a fixed number depending only on M and n , $\kappa > 0$ is also a fixed number depending only on n ; and

$$(4) \quad S(Q, \pi^\nu, \pi'^\nu, M) := \left\{ \gamma \in \mathrm{SL}_n(\mathbb{Z}[i]) \cdot \mathrm{diag}(1, \pi^\nu, \dots, \pi^\nu, \pi^\nu \pi'^\nu) \cdot \mathrm{SL}_n(\mathbb{Z}[i]) : \right. \\ \left. \| |\det \gamma|^{-\frac{2}{n}} \cdot \gamma^* Q \gamma - Q \|_\infty \leq \max(N(\pi)^{-M}, N(\pi')^{-M}) \right\}$$

with $Q := |\det g|^{2/n} \cdot (g^*)^{-1} g^{-1}$, and by $\|\cdot\|_\infty$ applied to a matrix, we mean its largest entry in absolute value. Note that in [BM15] and [BM16], the transpose of γ and g are taken instead of their adjoint.

By the prime number theorem, we can choose \mathcal{P} to satisfy $\#\mathcal{P} \gg_\varepsilon L^{1-\varepsilon}$ for any $\varepsilon > 0$. Therefore, if we were able to prove that

$$\#S(Q, \pi^\nu, \pi'^\nu, M) \ll_{\Omega, M} L^{\nu(n-1)-\eta}$$

holds for every $1 \leq \nu \leq n$ with some $\eta > 0$, then (3) would imply Theorem 1 by setting L to be a very small positive power of $D(\mu_\phi^*)$. We prove it in a weaker form, which still suffices for Theorem 1.

Before formulating this weaker statement, we fix some notation. Introduce the notation S_n for the real vector space of self-adjoint matrices in $\mathbb{C}^{n \times n}$ and $P_n \subset S_n$ for the open convex cone of positive definite matrices. Given a compact set $\Omega \subset X$ as in Theorem 1, we introduce

$$\Omega' := \left\{ \left[\frac{1}{2}, 2 \right] \cdot |\det g|^{\frac{2}{n}} \cdot (g^*)^{-1} g^{-1} : g \in \Omega \right\}.$$

Then Ω' is a compact subset of P_n in the subspace topology.

Proposition 1. *Let $\varepsilon > 0$ be arbitrary. There exist positive numbers $\alpha(\varepsilon) \geq 1$ and $M(\varepsilon) \geq 1$ (both depending only on n and ε) with the following properties. For any compact $\Omega \subset X$, there exists a constant $L(\Omega) \geq 2$ (depending only on n , $\alpha(\varepsilon)$, $M(\varepsilon)$ and Ω) such that the following holds. For any $L_0 \geq L(\Omega)$, there exists some $L_0 \leq L \leq L_0^{\alpha(\varepsilon)}$ such that for any prime π lying above a split rational prime and satisfying $L \leq N(\pi) < 2L$, we have*

$$(5) \quad \#S(Q, \pi^\nu, \pi^\nu, M(\varepsilon)) \ll_{\Omega, \varepsilon} L^{\nu(n-1)+\varepsilon}, \quad Q \in \Omega', 1 \leq \nu \leq n;$$

and for any two distinct primes π, π' lying above distinct split rational primes, we have

$$(6) \quad \#S(Q, \pi^\nu, \pi'^\nu, M(\varepsilon)) = 0, \quad Q \in \Omega', 1 \leq \nu \leq n.$$

This still suffices for the proof of Theorem 1. Indeed, we apply Proposition 1 with any $0 < \varepsilon < 1/2$. There are implied numbers $\alpha := \alpha(\varepsilon) \geq 1$ and $M := M(\varepsilon) \geq 1$, and together with the further input Ω , one more number $L(\Omega)$ by Proposition 1. Then take $L_0 := D(\mu_\phi^*)^\omega$, where $\omega > 0$ is a fixed constant to be specified later. By Proposition 1, if $L_0 \geq L(\Omega)$, we can find some with $D(\mu_\phi^*)^\omega \leq L \leq D(\mu_\phi^*)^{\alpha\omega}$ such that the countings (5) and (6) hold for any primes $L \leq N(\pi), N(\pi') < 2L$. Then in every term of (3), we get a power-saving, as soon as $\omega > 0$ in the beginning is chosen sufficiently small. Now we return to the condition $L_0 \geq L(\Omega)$. Apart from a finite set of Hecke–Maaß cusp forms depending only on Ω , this is indeed satisfied by $L_0 = D(\mu_\phi^*)^\omega$. The finitely many exceptional forms are treated then by adjusting the implied constant (note that the implied constant might depend on Ω , only the saving in the exponent must be absolute).

The rest of the paper is hence devoted to the proof of Proposition 1.

We conclude this section by illustrating why this counting problem is harder for $\mathrm{PGL}_n(\mathbb{Z}[i])$ than for $\mathrm{PGL}_n(\mathbb{Z})$ in the special case when Q is the unit matrix. Then in $S(\dots)$, we have a condition on the Smith normal form which is of the same complexity in both cases. However, the other condition is that γ is projectively equivalent to an orthonormal matrix, which intuitively happens more often over \mathbb{C} than over \mathbb{R} , since

$$\dim(\mathrm{PGL}_n(\mathbb{C})) = 2n^2 - 2, \quad \dim(\mathrm{PU}_n) = n^2 - 1 = \frac{\dim(\mathrm{PGL}_n(\mathbb{C}))}{2},$$

while

$$\dim(\mathrm{PGL}_n(\mathbb{R})) = n^2 - 1, \quad \dim(\mathrm{PO}_n) = \frac{n^2 - n}{2} < \frac{\dim(\mathrm{PGL}_n(\mathbb{R}))}{2},$$

i.e. PU_n is a “thicker” subgroup of $\mathrm{PGL}_n(\mathbb{C})$ than PO_n of $\mathrm{PGL}_n(\mathbb{R})$.

3. COUNTING TECHNIQUES IN A SPECIAL CASE

In this section, we introduce counting techniques for a situation which is very special in many different aspects. First, we will assume that Q is diagonal, moreover, its entries belong to the base field $\mathbb{Q}(i)$. Then these together imply that the diagonal entries are rational, i.e. $Q = \mathrm{diag}(q_1, \dots, q_n)$ with $q_1, \dots, q_n \in \mathbb{Q}$. Then $q_j \asymp_\Omega 1$ for all $1 \leq j \leq n$, and we also assume that the numerator and the denominator of q_j for all $1 \leq j \leq n$ (in their simplest form) are both coprime to π, π' . Our final simplification is that we allow no error term in (4), which we will denote by writing ∞ in place of M .

Our convention will be that vectors, i.e. elements of $\mathbb{Z}[i]^n, \mathbb{C}^n$, etc. are always meant as column vectors. We also introduce the notation $v_\pi(q)$, for any prime $\pi \in \mathbb{Z}[i]$ and any $q \in \mathbb{Q}(i)$, which denotes the π -valuation of q . Occasionally, we may use this notation for vectors or matrices with entries from $\mathbb{Q}(i)$, then it means the minimal π -adic valuation attained by the entries.

Lemma 1. *Let $\pi \in \mathbb{Z}[i]$ be a prime lying above a split rational prime $p = \pi\bar{\pi}$, $\rho \in \mathbb{N}$, and let $A \in \mathbb{Q}(i)^{n \times n}$ be a self-adjoint matrix such that $v_\pi(A) \geq 0$. Let $x = (\xi_1, \dots, \xi_n)^t, y = (v_1, \dots, v_n)^t \in \mathbb{Z}[i]^n$ be vectors satisfying $v_\pi(x) = v_\pi(y) = 0$ such that for any $1 \leq j < k \leq n$, $\pi^\rho \mid (\xi_j v_k - \xi_k v_j)$. Then the following statements hold.*

- (a) *For some $a \in \mathbb{Z}$ coprime to p , we have $y \equiv ax \pmod{\pi^\rho}$, and this a is well-defined modulo p^ρ .*
- (b) *Choosing $a \in \mathbb{Z}$ with this property in (a), there also exists a $b \in \mathbb{Z}$ (unique modulo p^ρ) with $b \equiv ai \pmod{\pi^\rho}$, so we further have*

$$(7) \quad 2x^*Ay \equiv (a - bi)x^*Ax + (a' - b'i)y^*Ay \pmod{p^\rho},$$

where $a' \in \mathbb{Z}$ (resp. $b' \in \mathbb{Z}$) stands for the multiplicative inverse of a (resp. of b) modulo p^ρ .

(c) We have $\pi^\rho \mid a' - b'i$ and $\overline{\pi}^\rho \mid a - bi$ for the integers a, b, a', b' defined above.

Proof. This is a variant of [BM16, Lemma 3], but the proof in this case is a little more computational. Without loss of generality, we may assume that $\pi \nmid \xi_n$. Then $\pi \nmid v_n$, for if not, then for some $1 \leq j \leq n-1$, $\pi \nmid v_j$, and then $\pi \nmid (\xi_n v_j - \xi_j v_n)$. Then $a \equiv v_n \xi_n^{-1} \pmod{\pi^\rho}$ does the job, since $v_j \equiv \xi_j v_n \xi_n^{-1} \equiv a \xi_j \pmod{\pi^\rho}$ for any $1 \leq j \leq n-1$. Also, a can be chosen in \mathbb{Z} uniquely modulo p^ρ since $0, 1, \dots, p^\rho - 1$ is a set of representatives modulo π^ρ (i.e. we have the isomorphism $\mathbb{Z}/(p^\rho) \cong \mathbb{Z}[i]/(\pi^\rho)$). The proof of (a) is complete.

As for (b), fix any representative $a \in \mathbb{Z}$ and let $b \in \mathbb{Z}$ be such that $b \equiv ai \pmod{\pi^\rho}$. Then π^ρ divides all the entries in $y - ax$ whence $\overline{\pi}^\rho$ divides all the entries in $(y - ax)^*$. So we deduce

$$0 \equiv (y - ax)^* A(y - ax) = y^* Ay + a^2 x^* Ax - ax^* Ay - ay^* Ax \pmod{p^\rho} = (\pi \overline{\pi})^\rho$$

hence

$$(8) \quad x^* Ay + y^* Ax \equiv ax^* Ax + a' y^* Ay \pmod{p^\rho}$$

where $a' \in \mathbb{Z}$ is a multiplicative inverse of a modulo p^ρ . Similarly, π^ρ divides all the entries in $iy - bx$ and $\overline{\pi}^\rho$ divides all the entries in $(iy - bx)^*$ as $ai \equiv b \pmod{\pi^\rho}$. So we compute

$$0 \equiv (iy - bx)^* A(iy - bx) = y^* Ay + b^2 x^* Ax - bix^* Ay + biy^* Ax \pmod{p^\rho}$$

whence

$$(9) \quad x^* Ay - y^* Ax \equiv -bix^* Ax - b'iy^* Ay \pmod{p^\rho}$$

where $b' \in \mathbb{Z}$ is a multiplicative inverse of b modulo p^ρ . The statement follows by adding equations (8) and (9).

For part (c), we compute $\pi^\rho \mid i(b - ai) = ib + a$ whence $\overline{\pi}^\rho \mid \overline{a + bi} = a - bi$. Similarly, $\pi^\rho \mid a'b'(b - ai) \equiv a' - b'i$. \square

Lemma 2. Let $A \in \Omega'$, and assume that $x_1, \dots, x_k \in \mathbb{Z}[i]^n$ are linearly independent vectors for some $0 \leq k \leq n-1$. Then for any real number $\beta \geq 2$,

$$\#\{y \in \mathbb{Z}[i]^n : y^* Ay = \beta^2, \text{ and } x_j^* Ay = 0 \text{ for any } j = 1, \dots, k\} \ll_{\Omega, \varepsilon} \beta^{2(n-k-1)+\varepsilon}$$

for any $\varepsilon > 0$.

Proof. See [BM15, Corollary 5.3]. \square

We slightly extend the notation $S(Q, \pi^\nu, \pi'^\nu, \infty)$ for $\pi, \pi' \nmid m \in \mathbb{Z}[i]$ as

$$S_m(Q, \pi^\nu, \pi'^\nu, \infty) := \left\{ \gamma \in \mathrm{SL}_n(\mathbb{Z}[i]_{\pi, \pi'}) \cdot \mathrm{diag}(1, \pi^\nu, \dots, \pi^\nu, \pi^\nu \pi'^\nu) \cdot \mathrm{SL}_n(\mathbb{Z}[i]_{\pi, \pi'}) : \right. \\ \left. m\gamma \in \mathrm{SL}_n(\mathbb{Z}[i]), |\det \gamma|^{-\frac{2}{n}} \cdot \gamma^* Q \gamma = Q \right\},$$

where by $\mathbb{Z}[i]_{\pi, \pi'}$, we mean the ring of elements $a \in \mathbb{Q}(i)$ which satisfy $v_\pi(a), v_{\pi'}(a) \geq 0$.

Lemma 3. Let $\pi \in \mathbb{Z}[i]$ be a prime lying above a split rational prime, and $\pi \nmid m \in \mathbb{Z}[i]$. Let $Q = \mathrm{diag}(q_1, \dots, q_n)$ with $q_j \in \mathbb{Q}$, $q_j \asymp_\Omega 1$ for all $1 \leq j \leq n$. Then for any $1 \leq \nu \leq n$,

$$\#S_m(Q, \pi^\nu, \pi'^\nu, \infty) \ll_{\Omega, \varepsilon} |m|^{2n^2-2+\varepsilon} \mathrm{den}(Q)^{\frac{(2n-1)(n-1)}{2}} N(\pi)^{\nu(n-1)+\varepsilon}.$$

for any $\varepsilon > 0$. Here, $\mathrm{den}(Q)$ denotes the least common multiple of the denominator of the diagonal entries of Q (written in simplest form).

Proof. By the definition of $S_m(Q, \pi^\nu, \pi'^\nu, \infty)$, any matrix counted there must have a column not completely divisible by π , and we may assume that it is the first column γ_1 . Since $(m\gamma_1)^* Q(m\gamma_1) = |m|^2 N(\pi)^\nu$, we have, by Lemma 2 that the number of possible $m\gamma_1$'s is $O_\varepsilon(|m|^{2(n-1)+\varepsilon} N(\pi)^{\nu(n-1)+\varepsilon})$. Now it suffices to prove that fixing γ_1 , there are $O_\Omega(m^{2n(n-1)} \mathrm{den}(Q)^{(2n-1)(n-1)/2})$ ways to finish the matrix.

We group the possible second columns γ_2 according to their π -valuation. When $v_\pi(\gamma_2) \geq \nu$, then $m\gamma_2/\pi^\nu \in \mathbb{Z}[i]^n$ and $\|m\gamma_2/\pi^\nu\| \asymp_\Omega \|m\gamma_2/\pi^\nu\|_Q = |m|$, hence there are $O_\Omega(|m|^{2n})$ such choices for such a γ_2 . Now fix $0 \leq \mu < \nu$, and then it suffices prove that the number of possible γ_2 's satisfying $v_\pi(\gamma_2) = \mu$ is $O_\Omega(|m|^{2n} \mathrm{den}(Q)^{(2n-1)/2})$, since the same can be repeated for all further columns.

Let x, y be second columns after the first column γ_1 such that $v_\pi(x) = v_\pi(y) = \mu$. Consider then the vectors $x' := mx/\pi^\mu$ and $y' := my/\pi^\mu$. By Lemma 1(a), x' and y' are both multiples of $m\gamma_1$ modulo $\pi^{\nu-\mu}$, and then by transitivity, multiples of each other modulo $\pi^{\mu-\nu}$. Introduce then $Q' := \text{den}(Q)Q$. With this notation, since $x'^*Q'x' = y'^*Q'y' = |m|^2q_2 \text{den}(Q)\pi^{\nu-\mu}\overline{\pi}^{\nu-\mu} = |m|^2q_2 \text{den}(Q)N(\pi)^{\nu-\mu}$, (7) gives that $x'^*Q'y'$ is divisible by $N(\pi)^{\nu-\mu}$. On the other hand, viewing \mathbb{C}^n as \mathbb{R}^{2n} , we obtain, for the Q -angle of x and y that

$$\angle_Q(x, y) = \arccos \frac{\Re(x^*Qy)}{\sqrt{(x^*Qx)(y^*Qy)}} = \arccos \frac{\Re(x'^*Q'y')}{\sqrt{(x'^*Q'x')(y'^*Q'y')}} = \arccos \frac{\Re(x'^*Q'y')}{|m|^2q_2 \text{den}(Q)N(\pi)^{\mu-\nu}}.$$

Since the numerator in the rightmost expression is divisible by $N(\pi)^{\mu-\nu}$, this continues, for some $\ell \in \{0, 1, 2, \dots\}$, as

$$\angle_Q(x, y) = \arccos \left(1 - \frac{\ell}{|m|^2q_2 \text{den}(Q)} \right) \gg_\Omega |m|^{-1} \text{den}(Q)^{-1/2}, \quad \text{if } \ell \neq 0, \text{ i.e. } x \neq y.$$

This means that the number of possible second columns is $O_\Omega(|m|^{2n-1} \text{den}(Q)^{(2n-1)/2})$ (this is rather elementary, see also [BM16, Lemma 4]). The proof is complete. \square

Lemma 4. *Let $\pi, \pi' \in \mathbb{Z}[i]$ be distinct primes lying above distinct split rational primes, and let $m \in \mathbb{Z}[i]$ such that $v_\pi(m) = v_{\pi'}(m) = 0$. Let further $Q = \text{diag}(q_1, \dots, q_n)$ such that $q_j \in \mathbb{Q}$ and $v_\pi(q_j) = v_{\pi'}(q_j) = 0$ for all $1 \leq j \leq n$. Then for any $1 \leq \nu \leq n$,*

$$\#S_m(Q, \pi^\nu, \pi'^\nu, \infty) = 0.$$

Proof. First observe that if $1 \leq \nu \leq n-1$, then

$$|\det \gamma|^{\frac{2}{n}} = (\pi\overline{\pi})^{\frac{\nu(n-1)}{n}} (\pi'\overline{\pi}')^{\frac{\nu}{n}} \notin \mathbb{Q},$$

hence $|\det \gamma|^{2/n} \gamma^* Q \gamma \neq Q$, implying $\#S_m(Q, \pi^\nu, \pi'^\nu, \infty) = 0$ in this case, so from now on, we assume $\nu = n$.

Any γ counted in $\#S_m(Q, \pi^n, \pi'^n, \infty)$ must have a column, say, the first one γ_1 such that $v_\pi(\gamma_1) = 0$. Now we prove that any choice of γ_2 leads to a contradiction. Let $\mu := v_\pi(\gamma_2) \geq 0$. Then we apply Lemma 1, in particular, (7) for γ_1 and $\gamma'_2 := \gamma_2/\pi^\mu$, with the notation $p = \pi\overline{\pi}$, $a, b \in \mathbb{Z}$ coprime to p such that $1 \leq a, b, a', b' \leq p^{n-\mu} - 1$, $\gamma'_2 \equiv a\gamma_1 \pmod{\pi^{n-\mu}}$, $b \equiv ai \pmod{\pi^{n-\mu}}$, a', b' are the multiplicative inverse of a, b modulo $p^{n-\mu}$, respectively. We infer

$$(10) \quad 0 = \pi^{-\mu} \gamma_1^* Q \gamma_2 = \gamma_1^* Q \gamma'_2 \equiv (a - bi)p^{n-1} \pi' \overline{\pi'} q_1 + (a' - b'i)p^{n-1-\mu} \pi' \overline{\pi'} q_2 \pmod{p^{n-\mu}},$$

which is immediately a contradiction for $\mu \geq 1$, since the second term in the rightmost expression is not divisible by $p^{n-\mu}$, while the first one and the sum are.

Now assume $\mu = 0$. By Lemma 1(c) we have $\pi \mid a - bi$ and $\pi \mid a' - b'i$. So in (10) the first term on the right-hand side is not divisible by π^n (since $\pi \nmid a - bi$ as $p \nmid a - bi$), while the second one and the sum are. \square

4. EXCHANGING MATRICES

Recall that we want to prove the countings (5) and (6) for $N(\pi), N(\pi') \in [L, 2L]$ with an appropriate choice of $L \geq L_0$ not exceeding a fixed power of L_0 . Our strategy is to switch Q for other matrices with better and better arithmetic properties. Note that a priori, Q is a point on a real manifold with entries that might be highly transcendental. We first informally describe these switches. First we will write Q_1 in place of Q in order to guarantee that

$$S(Q, \pi^\nu, \pi'^\nu, M) \subseteq S(Q_1, \pi^\nu, \pi'^\nu, \infty)$$

for every admissible choice of π, π', ν satisfying that $N(\pi), N(\pi')$ are between two fixed powers of L_0 . This new Q_1 will have entries in a number field $K \supseteq \mathbb{Q}(i)$. Using this Q_1 , we will be able to show that in an appropriate subinterval (again, the norms are between two fixed powers of L_0), all the γ 's correspond to $\pi = \pi'$ or $\nu = n$.

Secondly, in this subinterval, we will find a Q_2 , this time satisfying that

$$S(Q, \pi^\nu, \pi'^\nu, M) \subseteq S(Q_2, \pi^\nu, \pi'^\nu, \infty)$$

for every admissible choice of π, π', ν satisfying that $N(\pi), N(\pi')$ fall into an even shorter subinterval (again, between two powers of L_0). This new Q_2 will have entries in $\mathbb{Q}(i)$, and we will have a control on their height.

Finally, we will diagonalize Q_2 into Q_3 , again, with a control on the height of the entries, which necessarily will be rational. This diagonalization process will affect the counted γ 's themselves, but not their number, and we will have a good control on the possible denominators of the newly counted γ 's, i.e.

$$\#S(Q, \pi^\nu, \pi^{\nu'}, M) \leq \#S(Q_2, \pi^\nu, \pi^{\nu'}, \infty) \leq \#S_m(Q_3, \pi^\nu, \pi^{\nu'}, \infty)$$

for π, π', ν as above. Then to the rightmost count here, we will apply Lemmata 3–4, which in fact will be of the quality of (5) and (6).

Now we carry out this plan in detail. First we formulate a statement on effective computability. The field of algebraic numbers is denoted by $\overline{\mathbb{Q}}$. Given an algebraic number a , we define the complexity of a as

$$\text{comp}(a) := \inf_{\substack{a = \frac{b}{c} \\ b, c \in \mathcal{O}_{\mathbb{Q}(a)}}} \left(\max_{\sigma \in \text{Hom}_{\mathbb{Q}}(\mathbb{Q}(a), \mathbb{C})} |\sigma(b)| + \max_{\sigma' \in \text{Hom}_{\mathbb{Q}}(\mathbb{Q}(a), \mathbb{C})} |\sigma'(c)| \right) + 1$$

with $\mathcal{O}_{\mathbb{Q}(a)}$ standing for the ring of integers of $\mathbb{Q}(a)$.

Lemma 5. *Let a_1, \dots, a_m be algebraic numbers and put $K := \mathbb{Q}(a_1, \dots, a_m)$. Assume that $f : \overline{\mathbb{Q}}^m \rightarrow \overline{\mathbb{Q}}$ is a function of m variables that is computed altogether by t additions, subtractions, multiplications and divisions. Then we have*

$$\text{comp}(f(a_1, \dots, a_m)) \leq \left(\max_{1 \leq j \leq m} (\text{comp}(a_j)) \right)^{O_{m,t,\text{deg}(K:\mathbb{Q})}(1)}.$$

Proof. See the first paragraph of the proof of [BM16, Lemma 5]. □

Include Ω' in some Ω_1 which is still a compact subset of P_n in such a way that $\Omega' \subset \text{int}(\Omega_1)$. We make this inclusion in a well-defined way, say, Ω_1 is the set of self-adjoint, positive definite matrices of eigenvalues between $a/2$ and $2b$, where a, b are respectively the smallest and the largest eigenvalues of matrices in Ω' . Then $\text{dist}(\Omega', P_n \setminus \Omega_1) \gg_{\Omega} 1$, where by the distance of matrices, we mean the one induced by the maximum of the entrywise distance.

Given any matrix $\gamma \in \text{GL}_n(\mathbb{C})$, we define the following linear transformation $B_\gamma : S_n \rightarrow S_n$:

$$B_\gamma(A) := \gamma^* A \gamma - |\det(\gamma)|^{\frac{2}{n}} A, \quad A \in S_n.$$

For any $0 < C_1 < C_2$, we introduce the notation $\mathcal{P}(C_1, C_2)$ for the set of primes $\pi \in \mathbb{Z}[i]$ satisfying that $\Re \pi, \Im \pi > 0$ and $C_1 \leq N(\pi) < C_2$ (then in particular, elements of $\mathcal{P}(C_1, C_2)$ lie above distinct split rational primes). Another notation we introduce is $T \geq 1$, a fixed number depending only on n , which exceeds all the implicit constants in $O(1)$'s ever mentioned in the paper.

Lemma 6. *Let $D \geq 2$ and $E \geq 2$ be arbitrary. Then there exist some $M \geq 2$ (depending on n, D, E) and $L_1(\Omega) \geq 2$ (depending on n, D, E, M, Ω) such that the following holds. For any $Q \in \Omega'$, there exists some $1 \leq j \leq n^2 + 1$ satisfying that*

$$S(Q, \pi^\nu, \pi^{\nu'}, M) = \emptyset$$

for all $\pi, \pi' \in \mathcal{P}(2L_0^{(DE)^j}, 2L_0^{(DE)^{j+1}})$, unless $\pi = \pi'$ or $\nu = n$.

Proof. Fix $Q \in \Omega'$. For any $L_0 \geq 2$, consider the subspaces (for the moment, with some unspecified $M \geq 2$)

$$H_j := \bigcap_{\substack{\gamma \in S(Q, \pi^\nu, \pi^{\nu'}, M) \\ \pi, \pi' \in \mathcal{P}(L_0, 2L_0^{(DE)^j}) \\ 1 \leq \nu \leq n}} \ker B_\gamma, \quad j = 1, \dots, n^2 + 2.$$

Then $S_n \supseteq H_1 \supseteq \dots \supseteq H_{n^2+2} \supseteq \{0\}$ and $\dim(S_n) = n^2$ imply that $H_j = H_{j+1}$ for some $1 \leq j \leq n^2 + 1$. Fix the smallest such j . Since $\dim S_n - \dim H_j \leq n^2$, we in fact obtain H_j by intersecting only n^2 many $\ker B_\gamma$'s, say, $H_j = \bigcap_{\ell=1}^t \ker B_{\gamma_\ell}$ with some $t \leq n^2$. Since each entry of each such γ_ℓ has complexity $O_\Omega((L_0^{(DE)^j})^{O(1)})$, H_j is defined via a system of linear equations with entries from $K = \mathbb{Q}(i, \pi_1^{1/n}, \dots, \pi_{2n^2}^{1/n})$ of complexity $O_\Omega((L_0^{(DE)^j})^{O(1)})$ by Lemma 5 (since the linear system defining H_j can be computed in $O(1)$ steps from the used γ 's).

By assumption, $\text{dist}(Q, \ker B_\gamma) \ll L_0^{-M}$, where by dist , we mean the distance in S_n as a real vector space of dimension n^2 . We claim that this implies that $\text{dist}(Q, H_j) = O_\Omega((L_0^{(DE)^j})^{O(1)} L_0^{-M})$. Indeed, take basis matrices V_1, \dots, V_m of the linear span of the $(\ker B_{\gamma_\ell})^\perp$'s such that each $V_{\ell'}$ is in one of the $\ker B_{\gamma_\ell}$'s, its entries are in K of complexity $O_\Omega((L_0^{(DE)^j})^{O(1)})$ (this can be done, because such a basis can be computed from the γ_ℓ 's, and then Lemma 5 applies). Such a basis can be orthogonalized by Gram–Schmidt into V'_1, \dots, V'_m , and then

$$\text{dist}(Q, H_j) = \|\text{proj}_{H_j^\perp}(Q)\| = \left\| \sum_{\ell'=1}^m \frac{\langle Q, V'_{\ell'} \rangle}{\langle V'_{\ell'}, V'_{\ell'} \rangle} V'_{\ell'} \right\| = \left\| \sum_{\ell'=1}^m \frac{\sum_{\ell''=1}^m U_{\ell'\ell''} \langle Q, V_{\ell''} \rangle}{\langle V'_{\ell'}, V'_{\ell'} \rangle} V'_{\ell'} \right\|,$$

where U is the matrix standing for the Gram–Schmidt process. Since $\langle Q, V_{\ell''} \rangle \ll L_0^{-M}$ (because for every ℓ'' , we have $V_{\ell''} \in \ker B_{\gamma_\ell}$ for some ℓ), and all the coefficients (including the entries of U , by Lemma 5) are of complexity $O_\Omega((L_0^{(DE)^j})^{O(1)})$, we indeed see that $\text{dist}(Q, H_j) = O_\Omega((L_0^{(DE)^j})^{O(1)} L_0^{-M})$, applying Lemma 5 again.

Now if M is large enough, say,

$$(11) \quad M \geq T \cdot (DE)^{n^2+2} + 1,$$

where recall that $T \geq 1$ is an upper bound on all the implicit constants in $O(1)$'s ever mentioned in the paper, then $\text{dist}(Q, H_j) = O_\Omega(L_0^{-1})$ (since $j \leq n^2 + 1$, the exponent $n^2 + 2$ seems to be an overkill, but for a later reference, it is better to force M even a slightly larger). Then with the convenient choice of $L_1(\Omega) \geq 2$, if $L_0 \geq L_1(\Omega)$, then $H_j \cap \text{int } \Omega_1 \neq \emptyset$, in particular, $H_j \neq \{0\}$. Further, since H_j is defined over K , we may find and fix some $0 \neq Q_1 \in H_j$ with entries in K .

By the definition of H_j and its choice $H_j = H_{j+1}$, we have that for any $\pi, \pi' \in \mathcal{P}(L_0, 2L_0^{(DE)^{j+1}})$ and any $1 \leq \nu \leq n$,

$$S(Q, \pi^\nu, \pi'^\nu, M) \subseteq S(Q_1, \pi^\nu, \pi'^\nu, \infty).$$

Assume that $\gamma \in S(Q, \pi^\nu, \pi'^\nu, M)$ for some $\pi, \pi' \in \mathcal{P}(2L_0^{(DE)^j}, 2L_0^{(DE)^{j+1}})$. Since Q_1 has a nonzero entry, say, Q_{rs} , this implies via the last display that

$$\gamma_r^* Q_1 \gamma_s = |\det(\gamma)|^{\frac{2}{n}} Q_{rs},$$

where γ_r, γ_s stand for the r th and s th column of γ , respectively. Here, the left-hand side is in K , so is the right-hand side, which implies that $|\det(\gamma)|^{2/n} = (\pi \bar{\pi})^{\nu(n-1)/n} (\pi' \bar{\pi}')^{\nu/n} \in K$. By the independence of roots (a theorem of Besicovitch [Bes40]) and that K is defined by n th roots of primes of norm less than $2L^{(DE)^j}$, while primes in the definition of H_{j+1} have norms at least $2L^{(DE)^j}$, we see that $\pi = \pi'$ or $\nu = n$, and the proof is complete. \square

Lemma 7. *Let $D \geq 2$ be arbitrary, and assume that $E > D^{n^2+1}$. Let $M, L_1(\Omega) \geq 2$ be given by Lemma 6 and (11). For any $Q \in \Omega'$, and for the corresponding $j \leq n^2 + 1$ given by Lemma 6, there exists a self-adjoint matrix Q_2 with entries in $\mathbb{Q}(i)$ of complexity $O_\Omega((L_0^{D^k (DE)^j})^{O(1)})$ for some $k \in \{0, \dots, n^2\}$ such that for any $\pi, \pi' \in \mathcal{P}(2L_0^{D^k (DE)^j}, 2L_0^{D^{k+1} (DE)^j})$ and any $1 \leq \nu \leq n$,*

$$S(Q, \pi^\nu, \pi'^\nu, M) \subseteq S(Q_2, \pi^\nu, \pi'^\nu, \infty).$$

Proof. Define the subspaces

$$H'_k := \bigcap_{\substack{\gamma \in S(Q, \pi^\nu, \pi'^\nu, M) \\ \pi, \pi' \in \mathcal{P}(2L_0^{D^k (DE)^j}, 2L_0^{D^{k+1} (DE)^j}) \\ 1 \leq \nu \leq n}} \ker B_\gamma, \quad k = 0, \dots, n^2 + 1.$$

Then $S_n \supseteq H'_0 \supseteq \dots \supseteq H'_{n^2+1} \supseteq \{0\}$ and $\dim(S_n) = n^2$ imply that $H'_k = H'_{k+1}$ for some $1 \leq k \leq n^2$. Fix the smallest such k .

By our choice $D^{n^2+1} < E$ we have $2L_0^{(DE)^j} \leq 2L_0^{D^k (DE)^j} < 2L_0^{D^{k+1} (DE)^j} < 2L_0^{(DE)^{j+1}}$, so we may apply Lemma 6 to deduce $S(Q, \pi^\nu, \pi'^\nu, M) = \emptyset$ unless $\pi = \pi'$ or $\nu = n$. In particular, we have $|\det(\gamma)|^{2/n} = (\pi \bar{\pi})^{\nu(n-1)/n} (\pi' \bar{\pi}')^{\nu/n} \in \mathbb{Z}$ for all $\gamma \in S(Q, \pi^\nu, \pi'^\nu, M)$ in the definition of H'_k . Therefore all linear maps B_γ

in the definition of H'_k are defined over $\mathbb{Q}(i)$. As in the proof of Lemma 6, we find a matrix $Q_2 \in \text{int } \Omega_1 \cap H'_k$ with entries in $\mathbb{Q}(i)$ of complexity $O_\Omega((L_0^{D^k(DE)^j})^{O(1)})$ by Lemma 5 such that the conclusion holds. (Note that this is the point where we use the slightly stronger condition (11) put on M that it exceeds not only $(DE)^j \cdot O(1)$, but $D^k(DE)^j \cdot O(1)$.) \square

Lemma 8. *Let $D \geq 2$ be arbitrary, and let E be as in Lemma 7, then $M, L_1(\Omega)$ as given by Lemma 6. For any $Q \in \Omega_1$, let j, k be the numbers given also by Lemmata 6–7. There exists some $m \in \mathbb{Z}[i]$ of complexity $O_\Omega((L_0^{D^k(DE)^j})^{O(1)})$ and a matrix $U \in \text{SL}_n(\mathbb{Z}[i, \frac{1}{m}])$ with the following properties:*

- (a) *All entries of U and U^{-1} have complexity $O_\Omega((L_0^{D^k(DE)^j})^{O(1)})$.*
- (b) *$Q_3 := U^*Q_2U$ is diagonal with entries in \mathbb{Q} of complexity $O_\Omega((L_0^{D^k(DE)^j})^{O(1)})$ and lies in a compact subset $\Omega_2 \subset P_n$ depending only on Ω .*
- (c) *For any $\pi, \pi' \in \mathcal{P}(2L_0^{D^k(DE)^j}, 2L_0^{D^{k+1}(DE)^j})$ not dividing m , and any $1 \leq \nu \leq n$, we have*

$$\#S(Q_2, \pi^\nu, \pi'^\nu, \infty) \leq \#S_m(Q_3, \pi^\nu, \pi'^\nu, \infty).$$

Proof. We construct U in a way such that Q_3 is a Gram–Schmidt orthogonalized form of Q_2 , i.e.

$$Q_3 = U^*Q_2U,$$

where U is an $\binom{n}{2}$ long composition of elementary base changes $\text{id}_n + uE_{\ell_1\ell_2}$ for $\ell_1 \neq \ell_2$, where u is chosen to eliminate the entry at position ℓ_1, ℓ_2 (note that U is not canonically determined, since we can eliminate the elements in any order, fix one once for all). Noting that each entry of Q_2 has complexity $O_\Omega((L_0^{D^k(DE)^j})^{O(1)})$, this proves (a) by Lemma 5.

As for (b), first we claim that in a Gram–Schmidt step applied to a positive definite matrix, one diagonal entry decreases in absolute value, and all the others remain the same. It suffices to check this for 2×2 blocks, where we see the calculation

$$\begin{pmatrix} 1 & 0 \\ -\frac{b}{a} & 1 \end{pmatrix} \begin{pmatrix} a & b \\ -\bar{b} & c \end{pmatrix} \begin{pmatrix} 1 & -\frac{b}{a} \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & c - \frac{|b|^2}{a} \end{pmatrix}.$$

Here, $0 < c - |b|^2/a < c$, so the claim is proven.

As a result, when we diagonalize any element of Ω_1 , the resulting diagonal matrix cannot have entry larger than the largest eigenvalue in Ω_1 , say, λ . But then the smallest eigenvalue cannot be smaller than Δ/λ^{n-1} , where Δ is the smallest determinant attained in Ω_1 . Therefore, any Gram–Schmidt process applied to any element of Ω_1 leads to positive definite matrices with eigenvalues between Δ/λ^{n-1} and λ . The set of such matrices is a good choice for Ω_2 .

The rationality of Q_3 is obvious, since it is self-adjoint and with diagonal entries a priori in $\mathbb{Q}(i)$. Then observe that the matrix Q_3 is computed in $O(1)$ many steps from Q_2 , which verifies via Lemma 5 that the entries of Q_3 are indeed of complexity $O_\Omega((L_0^{D^k(DE)^j})^{O(1)})$. This proves (b).

Also, put $m := \text{den}(U^{-1})\text{den}(U)$ (which is $\text{den}(U)^2$, since $\det(U) = 1$). Then m can be computed in $O(1)$ steps, and referring to Lemma 5, we see that the complexity of m is $O_\Omega((L_0^{D^k(DE)^j})^{O(1)})$ as claimed. In particular, we have $mU^{-1}\gamma U \in \mathbb{Z}[i]^{n \times n}$ for any $\gamma \in \text{SL}_n(\mathbb{Z}[i])$.

Finally, if $\pi, \pi' \nmid m$, then the base change given by U does not alter the π - and π' -parts of the Smith normal form. Hence if $\gamma \in S(Q_2, \pi^\nu, \pi'^\nu, \infty)$, then

$$|\det(\gamma)|^{\frac{2}{n}} Q_3 = |\det(\gamma)|^{\frac{2}{n}} U^*Q_2U = U^*\gamma^*Q_2\gamma U = (U^{-1}\gamma U)^*U^*Q_2U(U^{-1}\gamma U) = (U^{-1}\gamma U)^*Q_3(U^{-1}\gamma U)$$

shows that $U^{-1}\gamma U \in S_m(Q_3, \pi^\nu, \pi'^\nu, \infty)$. Since the U -conjugation is a bijection, we obtain (c). \square

5. THE ENDGAME

Let $\varepsilon > 0$ be given as in the input of Proposition 1. Choose then $D \geq 2$ such that $D\varepsilon/2 > T + 1$, where recall that $T \geq 1$ is an upper bound on all implicit constants in $O(1)$'s ever mentioned in the paper. Let then $E \geq 2$ as needed in Lemma 7, and then $M \geq 2$ as implied by Lemma 6. This M will be the $M(\varepsilon)$ of Proposition 1.

Now let Ω , hence Ω' , Ω_1, Ω_2 be given. Let $L(\Omega)$ be large enough such that on the other hand $L(\Omega) \geq L_1(\Omega)$ of Lemmata 6–7, and on the other hand that for any $L_0 \geq L(\Omega)$, and any m implied by Lemma 8 (for any possible $1 \leq j \leq n^2 + 1$ and $0 \leq k \leq n^2$), $N(m) < L_0^{D^{k+1}(DE)^j}$, which can be achieved, since $N(m) = O_\Omega(L_0^{D^k(DE)^j})$. This in particular implies $\pi \nmid m$ for any $\pi \in \mathcal{P}(L_0^{D^{k+1}(DE)^j}, 2L_0^{D^{k+1}(DE)^j})$. Note that at this point none of j, k, m is fixed, but we have the claimed bounds and the non-divisibility relations on them.

Let then $Q \in \Omega'$ and $L_0 \geq L(\Omega)$ be arbitrary. Then there exist some $1 \leq j \leq n^2 + 1$ given by Lemma 6, $0 \leq k \leq n^2$ and Q_2 given by Lemma 7, Q_3 and $m \in \mathbb{Z}[i]$ given by Lemma 8 with the properties given there. Let then $L := L_0^{D^{k+1}(DE)^j}$, which satisfies the magnitude requirement of Proposition 1 that $L_0 \leq L \leq L_0^{\alpha(\varepsilon)}$, where $\alpha(\varepsilon)$ is a constant depending only on ε (we can take $\alpha(\varepsilon) = D^{n^2+1}(DE)^{n^2+1}$). For any $\pi, \pi' \in \mathcal{P}(L, 2L)$ and any $1 \leq \nu \leq n$, we have, combining Lemmata 7–8, that

$$\#S(Q, \pi^\nu, \pi'^\nu, M) \leq \#S(Q_2, \pi^\nu, \pi'^\nu, \infty) \leq \#S_m(Q_3, \pi^\nu, \pi'^\nu, \infty).$$

Therefore, it suffices to estimate the rightmost expression from above. We apply Lemma 4 for $\pi \neq \pi'$ to see the count is 0, which proves (6). When $\pi = \pi'$, then we apply Lemma 3 (with $\varepsilon/2$ written in place of ε there) to see it is

$$O_\Omega((L_0^{D^k(DE)^j})^{O(1)}) \cdot O_{\Omega, \varepsilon}((L_0^{D^{k+1}(DE)^j})^{\nu(n-1) + \frac{\varepsilon}{2}}) = O_{\Omega, \varepsilon}(L^{\nu(n-1) + \varepsilon}),$$

where the last bound holds by the choice of D and by $N(\pi) < 2L$. This proves (5).

The proof of Proposition 1 and hence that of Theorem 1 are complete.

REFERENCES

- [Bes40] A. S. Besicovitch. On the linear independence of fractional powers of integers. *J. London Math. Soc.*, 15:3–6, 1940.
- [BH10] V. Blomer and G. Harcos. Twisted L -functions over number fields and Hilbert’s eleventh problem. *Geom. Funct. Anal.*, 20(1):1–52, 2010.
- [BHM16] V. Blomer, G. Harcos, and D. Milićević. Bounds for eigenforms on arithmetic hyperbolic 3-manifolds. *Duke Math. J.*, 165(4):625–659, 2016.
- [BHMM20] V. Blomer, G. Harcos, P. Maga, and D. Milićević. The sup-norm problem for $GL(2)$ over number fields. *J. Eur. Math. Soc. (JEMS)*, 22(1):1–53, 2020.
- [BM15] V. Blomer and P. Maga. The sup-norm problem for $PGL(4)$. *Int. Math. Res. Not. IMRN*, (14):5311–5332, 2015.
- [BM16] V. Blomer and P. Maga. Subconvexity for sup-norms of cusp forms on $PGL(n)$. *Selecta Math. (N.S.)*, 22(3):1269–1287, 2016.
- [BP16] V. Blomer and A. Pohl. The sup-norm problem on the Siegel modular space of rank two. *Amer. J. Math.*, 138(4):999–1027, 2016.
- [BT20] F. Brumley and N. Templier. Large values of cusp forms on GL_n . *Selecta Math. (N.S.)*, 26(4):Paper No. 63, 71, 2020.
- [Gil20] N. Gillman. Explicit subconvexity savings for sup-norms of cusp forms on $PGL_n(\mathbb{R})$. *J. Number Theory*, 206:46–61, 2020.
- [GRS13] A. Ghosh, A. Reznikov, and P. Sarnak. Nodal domains of Maass forms I. *Geom. Funct. Anal.*, 23(5):1515–1568, 2013.
- [IS95] H. Iwaniec and P. Sarnak. L^∞ norms of eigenfunctions of arithmetic surfaces. *Ann. of Math. (2)*, 141(2):301–320, 1995.
- [Mar] S. Marshall. Upper bounds for Maass forms on semisimple groups. Available at <https://arxiv.org/abs/1405.7033>.
- [RS94] Z. Rudnick and P. Sarnak. The behaviour of eigenstates of arithmetic hyperbolic manifolds. *Comm. Math. Phys.*, 161(1):195–213, 1994.
- [Sar] P. Sarnak. Letter to Morawetz. Available at http://publications.ias.edu/sites/default/files/Sarnak_Letter_to_Morawetz.pdf.

ALFRÉD RÉNYI INSTITUTE OF MATHEMATICS, HUNGARIAN ACADEMY OF SCIENCES, POB 127, BUDAPEST H-1364, HUNGARY
Email address: magapeter@gmail.com, gergely.zabradi@ttk.elte.hu

EÖTVÖS LORÁND UNIVERSITY, INSTITUTE OF MATHEMATICS, PÁZMÁNY PÉTER SÉTÁNY 1/C, BUDAPEST H-1117, HUNGARY
Email address: gergely.zabradi@ttk.elte.hu