HAL open science

Moments in the Chebotarev density theorem: non-Gaussian families

Régis de La Bretèche, Daniel Fiorilli, Florent Jouve

To cite this version:

Régis de La Bretèche, Daniel Fiorilli, Florent Jouve. Moments in the Chebotarev density theorem: non-Gaussian families. 2023. hal-03961992

HAL Id: hal-03961992

https://inria.hal.science/hal-03961992v1

Preprint submitted on 29 Jan 2023

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

MOMENTS IN THE CHEBOTAREV DENSITY THEOREM: NON-GAUSSIAN FAMILIES

RÉGIS DE LA BRETÈCHE, DANIEL FIORILLI, AND FLORENT JOUVE

À la mémoire de Joël Bellaïche

Abstract. In this paper we investigate higher moments attached to the Chebotarev Density Theorem. Our focus is on the impact that peculiar Galois group structures have on the limiting distribution. Precisely we consider in this paper the case of groups having a character of large degree. Under the Generalized Riemann Hypothesis, we prove in particular that there exists families of Galois extensions of number fields having doubly transitive Frobenius group for which no Gaussian limiting distribution occurs.

1. Introduction

Let L/K be a Galois extension of number fields, $G = \mathrm{Gal}(L/K)$ and let $t\colon G \to \mathbb{R}$ be a class function. The goal of this paper is twofold: we wish to understand the moments of the variance as well as the average of the n-th moment (those quantities will be precisely defined in (3) and (6) respectively) of the prime counting function

$$\psi_\eta(x; L/K, t) := \sum_{\substack{\mathfrak{p} \lhd \mathcal{O}_K \\ m \geq 1}} t(\varphi_\mathfrak{p}^m) \frac{\log(\mathcal{N}\mathfrak{p})}{\mathcal{N}\mathfrak{p}^{\frac{m}{2}}} \eta\big(\log(\mathcal{N}\mathfrak{p}^m/x)\big)\,, \tag{1}$$

assuming that G has an irreducible representation of very large degree. The reason why we are interested in those groups is that, as we will see, they give rise to non-Gaussian moments, in contrast with what was obtained in the cyclotomic case [2] (more precisely, $K = \mathbb{Q}$, $L = \mathbb{Q}(\zeta_q)$ and $t = \mathbf{1}_{1 \bmod q} - \frac{1}{\phi(q)}$). In (1), $\varphi_\mathfrak{p}$ (resp. $\mathcal{N}\mathfrak{p}$) denotes the Frobenius at (resp. the norm of) the prime ideal $\mathfrak{p}$ (see [3, (3)] for details on the ramified case) and η is a weight function satisfying properties which we now recall.

We let $\delta > 0$ and $\mathcal{S}_\delta \subset \mathcal{L}^1(\mathbb{R})$ be the set of all non-trivial differentiable even $\eta\colon \mathbb{R} \to \mathbb{R}$ such that for all $t \in \mathbb{R}$,

$$\eta(t), \eta'(t) \ll \mathrm{e}^{-(\frac{1}{2}+\delta)|t|},$$

and moreover for all $\xi \in \mathbb{R}$, we have that

$$0 \leq \widehat{\eta}(\xi) \ll (|\xi|+1)^{-1}(\log(|\xi|+2))^{-2-\delta}. \tag{2}$$

Here, the Fourier transform is defined by

$$\widehat{\eta}(\xi) := \int_\mathbb{R} \mathrm{e}^{-2\pi i \xi u} \eta(u) \mathrm{d}u\,.$$

Date: January 28, 2023.

Finally for any $h \in \mathcal{L}^1(\mathbb{R})$ we define

$$\alpha(h) := \int_{\mathbb{R}} h(t)\,\mathrm{d}t\,.$$

First we notice that, with the smooth weight $\eta \in \mathcal{S}_\delta$, the Chebotarev density theorem reads

$$\psi_\eta(x; L/K, t) \sim \widehat{t}(1) x^{\frac{1}{2}} \mathcal{L}_\eta(\tfrac{1}{2}),$$

where, denoting by $\mathrm{Irr}(G)$ the set of irreducible complex representations of G, we define

$$\widehat{t}(\chi) := \langle t, \chi\rangle_G = \frac{1}{|G|}\sum_{g\in G} t(g)\overline{\chi(g)}\,, \qquad \mathcal{L}_\eta(u) := \int_{\mathbb{R}} \mathrm{e}^{ux}\eta(x)\mathrm{d}x \qquad (\chi \in \mathrm{Irr}(G)).$$

Note that $\mathcal{L}_\eta(u) = \mathcal{L}_\eta(-u)$. Secondly, it follows from an analysis as in [5, Proposition 3.18] that under the Riemann Hypothesis for all Artin L-functions $L(s, L/K, \chi)$ (an assumption that will be denoted GRH throughout the paper), the remainder term $\psi_\eta(x; L/K, t) - \widehat{t}(1)x^{\frac{1}{2}}\mathcal{L}_\eta(\frac{1}{2})$ has average value equal to $\widehat{\eta}(0)z(L/K, t)$, where we define

$$z(L/K, t) := \sum_{\chi\in\mathrm{Irr}(G)} \widehat{t}(\chi)\mathrm{ord}_{s=\frac{1}{2}} L(s, L/K, \chi)\,.$$

For $\eta \in \mathcal{S}_\delta$, and $u \geq 0$, we consider the n-th moment

$$\mathcal{M}_n(u; L/K, \eta) := \frac{1}{|G|}\sum_{C\in G^\sharp} |C|\Big(\frac{|G|}{|C|}\psi_\eta(\mathrm{e}^u; L/K, 1_C) - \mathrm{e}^{\frac{u}{2}}\mathcal{L}_\eta(\tfrac{1}{2}) - \widehat{\eta}(0)z(L/K, \tfrac{|G|}{|C|}1_C)\Big)^n,$$

where $G^\sharp$ is the set of conjugacy classes of G. Note that for $t_C = \frac{|G|}{|C|}1_C$, we have that $\widehat{t_C}(\chi) = \overline{\chi(C)}$ and thus $z(L/K, \frac{|G|}{|C|}1_C) \in \mathbb{R}$ (by the functional equation satisfied by $L(s, L/K, \chi)$). Equivalently, we may take the average over all $g \in G$ of the n-th power of the error term in the Chebotarev density theorem corresponding to the conjugacy class C_g of g. We define $\mathcal{U}$ to be the set of even non-trivial integrable functions $\Phi\colon \mathbb{R} \to \mathbb{R}$ such that $\Phi, \widehat{\Phi} \geq 0$, and we consider for $U > 0$, $\Phi \in \mathcal{U}$, $\eta \in \mathcal{S}_\delta$, $n = 2$ and $s \in \mathbb{N}$, the moments

$$\mathcal{V}_{2,s}(U; L/K, \Phi, \eta) := \frac{1}{U\int_0^\infty \Phi}\int_0^\infty \Phi(\tfrac{u}{U})\Big(\mathcal{M}_2(u; L/K, \eta) - m_2(L/K; \eta)\Big)^s \mathrm{d}u\,, \tag{3}$$

where

$$m_2(L/K; \eta) := \lim_{U\to\infty}\frac{1}{U}\int_2^U \mathcal{M}_2(u; L/K, \eta)\mathrm{d}u.$$

We will show that under Artin's holomorphy conjecture for $L(s, L/K, \chi)$ for all non-trivial $\chi \in \mathrm{Irr}(G)$ (which we will denote by AC) and GRH, the integral in (3) converges and the limit defining m_2 exists.

The goal of this paper is to study the special case when $\mathrm{Irr}(G)$ has one dominant character, that is there exists $\vartheta \in \mathrm{Irr}(G)$ such that $\vartheta(1) \sim |G|^{\frac{1}{2}}$. Note that as soon as $2\vartheta(1)^2 > |G|$, the character ϑ is necessarily real. We introduce the following notation:

$$\lambda_j(G) := \sum_{\chi\in\mathrm{Irr}(G)} \chi(1)^j\,, \qquad (j \geq 1)\,.$$

Our first main result establishes a lower bound on the s-th moment of the variance (3). We let

$$\mu_0 := 1\,, \qquad \mu_r := \begin{cases} (2n-1)\cdot(2n-3)\cdots 1 & \text{if } r = 2n \geq 2, \\ 0 & \text{if } r = 2n+1. \end{cases}$$

denote r-th moment of the Gaussian, and for a number field L, we let $\mathrm{rd}_L := d_L^{\frac{1}{[L:\mathbb{Q}]}}$, where d_L is the absolute value of the absolute discriminant of L.

Theorem 1.1. *Let L/K be a Galois extension and assume AC and GRH. Let $\eta \in \mathcal{S}_\delta$ and $\Phi \in \mathcal{U}$. Assume moreover that there exists a (necessarily real) character $\vartheta \in \mathrm{Irr}(G)$ such that $|G| - f(|G|) \leq \vartheta(1)^2 \leq |G| - 1$ where f is a function such that $1 \leq f(|G|) \leq \frac{1}{4}|G|$. Then for $s \in \mathbb{N}$ and $U \geq 1$ we have the estimate*

$$\mathcal{V}_{2,s}(U; L/K, \Phi, \eta) \geq H_s\big(\alpha(|\widehat{\eta}|^2)[K:\mathbb{Q}]|G|^{\frac{1}{2}}\log(\mathrm{rd}_L)\big)^s\Big(1 + O\Big(\frac{sf(G)^{\frac{1}{2}}}{|G|^{\frac{1}{2}}} + \frac{s^2}{\log\log(\mathrm{rd}_L+2)}\Big)\Big) + O\Big(\frac{(\kappa_\eta[K:\mathbb{Q}]^2(\log(\mathrm{rd}_L+2))^2\lambda_1(G)^2)^s}{U}\Big),$$

where

$$H_s := \sum_{j=0}^{s}\binom{s}{j}(-1)^{s-j}\mu_{2j}, \tag{4}$$

and where $\kappa_\eta > 0$ is a constant which depends on η.

Remark. The quantity H_s is the s-th moment of $Z^2 - 1$, where $Z \sim \mathcal{N}(0,1)$, the standard Gaussian. Indeed, the s-th moment of $Z^2 - 1$ is equal to

$$\mathbb{E}\big[(Z^2-1)^s\big] = \frac{1}{\sqrt{2\pi}}\int_{\mathbb{R}}(t^2-1)^s\mathrm{e}^{-\frac{t^2}{2}}\mathrm{d}t = \sum_{j=0}^{s}\binom{s}{j}(-1)^{s-j}\frac{1}{\sqrt{2\pi}}\int_{\mathbb{R}}t^{2j}\mathrm{e}^{-\frac{t^2}{2}}\mathrm{d}t = H_s.$$

Note that $H_1 = 0$ and morever $H_{2k+1} > 0$ for all $k \geq 1$ (this follows from the recurrence $H_{s+2} = 2(s+1)(H_{s+1} + H_s)$ for $s \in \mathbb{N}$).

We now give an intuitive reason why we should expect the moments H_s in Theorem 1.1. By Parseval's identity, we have that

$$\mathcal{M}_2(u; L/K, \eta) = \sum_{\chi \in \mathrm{Irr}(G)}\big|\psi_\eta(\mathrm{e}^u; L/K, \chi) - \mathrm{e}^{\frac{u}{2}}\mathcal{L}_\eta(\tfrac{1}{2}) - \widehat{\eta}(0)\mathrm{ord}_{s=\frac{1}{2}}L(s, L/K, \chi)\big|^2. \tag{5}$$

We expect this sum to be dominated by the term for the character $\chi = \vartheta$ of large degree. Moreover, we expect $\psi_\eta(\mathrm{e}^u; L/K, \chi) - \mathrm{e}^{\frac{u}{2}}\mathcal{L}_\eta(\frac{1}{2}) - \widehat{\eta}(0)\mathrm{ord}_{s=\frac{1}{2}}L(s, L/K, \chi)$ to have Gaussian moments (see [5], [3]), hence we expect $\mathcal{M}_2(u; L/K, \eta)$ to be approximately the square of a Gaussian. As a result, we expect $\mathcal{V}_{2,s}(U; L/K, \Phi, \eta)$ to be the centered moments of the square of a Gaussian, which is what we obtain.

In addition to computing the higher centered moments of the variance $\mathcal{M}_2(u; L/K, \eta)$, we also compute the first moment of all moments $\mathcal{M}_n(u; L/K, \eta)$ for particular non-abelian Galois groups G. More precisely we will be interested in the moment

$$M_{n,1}(U; L/K, \Phi, \eta) := \frac{1}{U\int_0^\infty \Phi}\int_0^\infty \Phi(\tfrac{u}{U})\mathcal{M}_n(u; L/K, \eta)\mathrm{d}u. \tag{6}$$

The cyclotomic case where $G \simeq (\mathbb{Z}/q\mathbb{Z})^\times$ was studied in [1]; in this context we expect to have Gaussian moments. Our next result focuses on the case where the group G has order $d(d+1)$ for some integer $d \geq 2$, and where G admits an irreducible representation of degree d (specifically G is a doubly transitive Frobenius group as defined *e.g.* in [7, Prop. 6.5]). We will show that for this family of groups, the associated moments are not necessarily Gaussian.

Theorem 1.2. *Let G be a doubly transitive Frobenius group of order $d(d+1) \geq 6$ with kernel N and abelian complement H. Let L/K be a Galois extension of number fields of group G and assume GRH. Let $\eta \in \mathcal{S}_\delta$ an $\Phi \in \mathcal{U}$. Then for $m \in \mathbb{N}$ and $U \geq 1$ we have the estimate*

$$M_{2m,1}(U; L/K, \Phi, \eta) \geq \frac{\mu_{2m} d^{2m}}{d(d+1)} \widehat{\eta}^{2m}(0) \Big((d-1)[K:\mathbb{Q}] \log(\mathrm{rd}_L) \Big)^m \Big(1 + O\Big(\frac{m}{\log(\mathrm{rd}_L + 2)} \Big) \Big) + O\big(U^{-1} (d+1)^{4m-2} ([K:\mathbb{Q}] \log(\mathrm{rd}_L + 2))^{2m} \big). \tag{7}$$

Moreover, in the limit as $U \to \infty$, the normalized moment

$$M_{2m,1}(U; L/K, \Phi, \eta) / M_{2,1}(U; L/K, \Phi, \eta)^m$$

is asymptotically at least[1] $\mu_{2m} d^{m-2} / ([K:\mathbb{Q}] \log(\mathrm{rd}_L))^m (1 + o_{d\to\infty}(1))$ *(and is therefore non-Gaussian as soon as $[K:\mathbb{Q}] \log(\mathrm{rd}_L) = o(d^{1-\varepsilon})$ for some fixed $\varepsilon > 0$).*

To obtain an explicit non-Gaussian family, consider the extension (see Example 1) $K = \mathbb{Q}$, $L = \mathbb{Q}(a^{\frac{1}{p}}, \zeta_p)$ where a, p are primes such that $p^2 \nmid a^{p-1} - 1$ (there is a sequence of such pairs (a, p) with both a, p tending to infinity; see [5, Lemma 9.9]), one has that $\log(\mathrm{rd}_L) \ll \log(ap)$ and $d = p - 1$ (see [5, Prop. 9.8]). We conclude that $[K:\mathbb{Q}] \log(\mathrm{rd}_L) = o(d^{1-\varepsilon})$, and thus Theorem 1.2 implies that we have non-Gaussian moments.

Remark. All the irreducible representations of a doubly transitive Frobenius group G are monomial (*i.e.* induced from a representation of degree 1 of a subgroup, see Corollary 3.3). In particular Brauer's Theorem implies that AC holds for any Galois extension of number fields whose Galois group is isomorphic to G.

The paper is organized as follows. In §2 we prove Theorem 1.1 by first establishing a few preparatory results about properties of H_s as well as bounds on certain Artin conductors. We devote §3 to the proof of Theorem 1.2 which exploits specific properties of doubly transitive Frobenius groups.

2. Moments of the variance: Proof of Theorem 1.1

Let us first give a precise bound on the Artin conductor $A(\vartheta)$ (see *e.g.* [3, §3] for recollections on Artin conductors in this context) of the dominant character ϑ appearing in Theorem 1.1.

Lemma 2.1. *Let L/K be a Galois extension of number fields of group G where $|G| \geq 4$, and assume that there exists $\vartheta \in \mathrm{Irr}(G)$ such that $|G| - f(|G|) \leq \vartheta(1)^2 \leq |G| - 1$, where f is a function such that $1 \leq f(|G|) \leq \frac{1}{4}|G|$. Then we have the bounds*

$$1 - \frac{f(|G|)^{\frac{1}{2}}}{|G|^{\frac{1}{2}}} - 2\frac{f(|G|)^{\frac{3}{2}}}{|G|^{\frac{3}{2}}} \leq \frac{\log(A(\vartheta))}{\vartheta(1)[K:\mathbb{Q}] \log(\mathrm{rd}_L)} \leq 1 + \frac{f(|G|)^{\frac{1}{2}}}{|G|^{\frac{1}{2}}} + 2\frac{f(|G|)^{\frac{3}{2}}}{|G|^{\frac{3}{2}}}.$$

[1] Note that we expect the "true size" of this moment to be asymptotically $\mu_{2m} d^{2m}$.

Proof. Since

$$1 = \langle \vartheta, \vartheta \rangle_G = \frac{\vartheta(1)^2}{|G|} + \frac{1}{|G|} \sum_{1 \neq g \in G} \vartheta(g)\overline{\vartheta(g)},$$

it follows that for all $g \neq 1$,

$$|\vartheta(g)| \leq f(|G|)^{\frac{1}{2}} \leq \vartheta(1) \frac{f(|G|)^{\frac{1}{2}}}{|G|^{\frac{1}{2}}} \Big(1 + 2\frac{f(|G|)}{|G|}\Big).$$

As a result, [5, Lemma 4.2] implies the claimed bounds. □

Remark. Writing $d = \vartheta(1)$, we have $|G| = d(d+e)$ for some $e \geq 1$ (see the beginning of §3). As a result, in Lemma 2.1 one necessarily has $f(|G|) \geq de \geq |G|^{\frac{1}{2}} - \frac{1}{2}$.

We will need the following combinatorial result.

Lemma 2.2. *Fix $s \in \mathbb{N}$ and let $\mathcal{H}_s$ be the set of involutions $\pi : \{1, \ldots, s\} \times \{1, 2\} \to \{1, \ldots, s\} \times \{1, 2\}$ having no fixed point and such that $\pi(j, 1) \neq (j, 2)$ for all $j \leq s$. Then we have $|\mathcal{H}_s| = H_s$, where H_s is defined by (4).*

Remark. As $s \to \infty$, we have the asymptotic formula

$$H_s = (\mathrm{e}^{-1/2} + o(1))\mu_{2s}.$$

Proof of Lemma 2.2. We first prove the relation

$$\sum_{k=0}^{s} \binom{s}{k} |\mathcal{H}_{s-k}| = \mu_{2s}, \tag{8}$$

from which the claimed identity follows. Consider the set of involutions $\pi : \{1, \ldots, s\} \times \{1, 2\} \to \{1, \ldots, s\} \times \{1, 2\}$ having no fixed points; the total number of such involutions is μ_{2s}. This set can be partitioned according to the number k of $1 \leq j \leq s$ such that $\pi(j, 1) = (j, 2)$. The number of elements in each of these subsets is equal to $\binom{s}{k}|\mathcal{H}_{s-k}|$, thus we obtain the claimed identity. The proof is finished. □

The next step will be to apply the explicit formula and bound $\mathcal{V}_{2,s}(U; L/K, \Phi, \eta)$ in terms of the quantity

$$\mathbb{V}_{2,s}(L/K; \eta) := \sum_{\chi_1, \ldots, \chi_s \in \mathrm{Irr}(G)} \sum_{\substack{\gamma_{\chi_1}, \gamma'_{\chi_1}, \ldots, \gamma_{\chi_s}, \gamma'_{\chi_s} \neq 0 \\ \gamma_{\chi_j} \neq \gamma'_{\chi_j} \\ \sum_{j=1}^{s} (\gamma_{\chi_j} - \gamma'_{\chi_j}) = 0}} \prod_{j=1}^{s} \Big(\widehat{\eta}\Big(\frac{\gamma_{\chi_j}}{2\pi}\Big)\widehat{\eta}\Big(\frac{\gamma'_{\chi_j}}{2\pi}\Big)\Big), \tag{9}$$

where γ_{χ_j} and γ'_{χ_j} run through the imaginary parts of the non-trivial zeros of $L(s, L/K, \chi_j)$.

Lemma 2.3. *Fix $s \in \mathbb{N}$ and let L/K be a Galois extension and assume AC and GRH. Let $\eta \in \mathcal{S}_\delta, \Phi \in \mathcal{U}$. Then for $U \geq 1$ we have the estimate*

$$\mathcal{V}_{2,s}(U; L/K, \Phi, \eta) \geq \mathbb{V}_{2,s}(L/K; \eta) + O\Big(\frac{(\kappa_\eta [K : \mathbb{Q}]^2 (\log(\mathrm{rd}_L + 2))^2 \lambda_1(G)^2)^s}{U}\Big),$$

where $\kappa_\eta > 0$ is a constant which depends on η.

Proof. By [3, Lemma 4.1], we have that

$$\frac{|G|}{|C|}\psi_\eta(\mathrm{e}^u; L/K, 1_C) - \mathrm{e}^{\frac{u}{2}}\mathcal{L}_\eta(\tfrac{1}{2}) - \widehat{\eta}(0)z(L/K, t_C) = -\sum_{\chi\in\mathrm{Irr}(G)} \overline{\chi}(C) \sum_{\rho_\chi\notin\mathbb{R}} \mathrm{e}^{i\gamma_\chi u}\widehat{\eta}\Big(\frac{\gamma_\chi}{2\pi}\Big) + O\Big(\mathrm{e}^{-\frac{u}{2}}[K:\mathbb{Q}]\lambda_{1,1}(t_C)\log(\mathrm{rd}_L+2)\Big),$$

where $\lambda_{1,1}(t_.)\colon G^\sharp \to \mathbb{R}$ is defined by $\lambda_{1,1}(t_C) = \sum_{\chi\in\mathrm{Irr}(G)} \chi(1)|\widehat{t_C}(\chi)|$ (recall $t_C = \frac{|G|}{|C|}1_C$).

Note that the main term here satisfies the bound

$$\sum_{\chi\in\mathrm{Irr}(G)} \overline{\chi}(C) \sum_{\rho_\chi\notin\mathbb{R}} \mathrm{e}^{i\gamma_\chi u}\widehat{\eta}\Big(\frac{\gamma_\chi}{2\pi}\Big) \ll [K:\mathbb{Q}]\lambda_{1,1}(t_C)\log(\mathrm{rd}_L+2),$$

by the Riemann-von Mangoldt formula [8, Theorem 5.8]. By the orthogonality of irreducible characters, we deduce that

$$\mathcal{M}_2(u; L/K, \eta) = \sum_{\chi\in\mathrm{Irr}(G)} \sum_{\gamma_\chi,\gamma'_\chi\notin\mathbb{R}} \mathrm{e}^{i(\gamma_\chi-\gamma'_\chi)u}\widehat{\eta}\Big(\frac{\gamma_\chi}{2\pi}\Big)\widehat{\eta}\Big(\frac{\gamma'_\chi}{2\pi}\Big) + O\Big(\mathrm{e}^{-\frac{u}{2}}\frac{[K:\mathbb{Q}]^2(\log(\mathrm{rd}_L+2))^2}{|G|}\sum_{C\in G^\sharp}|C|\lambda_{1,1}(t_C)^2\Big),$$

which implies in particular that

$$m_2(L/K;\eta) = \sum_{\chi\in\mathrm{Irr}(G)} b_0^+(\chi; |\widehat{\eta}|^2),$$

with

$$b_0^+(\chi; h) := \sum_{\rho_\chi\notin\mathbb{R}} \mathrm{ord}_{s=\rho_\chi} L(s, L/K, \chi) h\Big(\frac{\rho_\chi - \frac{1}{2}}{2\pi i}\Big). \tag{10}$$

Note also that

$$\sum_{C\in G^\sharp}|C|\lambda_{1,1}(t_C)^2 = \frac{1}{|G|}\sum_{C\in G^\sharp}|C|\Big(\sum_{\chi\in\mathrm{Irr}(G)}\chi(1)|\chi(C)|\Big)^2 \le \Big(\sum_{\chi\in\mathrm{Irr}(G)}\chi(1)\Big)^2 = \lambda_1(G)^2\,.$$

We then have the following bound for the main term in our estimate for $\mathcal{M}_2(u; L/K, \eta)$:

$$\sum_{\chi\in\mathrm{Irr}(G)} \sum_{\gamma_\chi,\gamma'_\chi\neq 0} \mathrm{e}^{i(\gamma_\chi-\gamma'_\chi)u}\widehat{\eta}\Big(\frac{\gamma_\chi}{2\pi}\Big)\widehat{\eta}\Big(\frac{\gamma'_\chi}{2\pi}\Big) \ll \sum_{\chi\in\mathrm{Irr}(G)}(\log A(\chi))^2 \ll [K:\mathbb{Q}]^2(\log(\mathrm{rd}_L+2))^2|G|,$$

where we have used [3, Lemma 4.2] as well as [5, Lemma 4.1]. Expanding the s-th power, we deduce that

$$\begin{aligned}
&\mathcal{V}_{2,s}(U;L/K,\Phi,\eta)\\
&\quad=\frac{2}{U\widehat{\Phi}(0)}\int_0^\infty \Phi(\tfrac{u}{U})\Big(\sum_{\chi\in\mathrm{Irr}(G)}\sum_{\substack{\gamma_\chi,\gamma'_\chi\neq 0\\ \gamma_\chi\neq\gamma'_\chi}} \mathrm{e}^{i(\gamma_\chi-\gamma'_\chi)u}\widehat{\eta}\Big(\frac{\gamma_\chi}{2\pi}\Big)\widehat{\eta}\Big(\frac{\gamma'_\chi}{2\pi}\Big)\\
&\qquad\qquad+O\Big(\mathrm{e}^{-\frac{u}{2}}\big([K:\mathbb{Q}]\log(\mathrm{rd}_L+2)\lambda_1(G)^2\big)^2\Big)\Big)^s\mathrm{d}u,\\
&\quad=\frac{1}{\widehat{\Phi}(0)}\sum_{\chi_1,\dots,\chi_s\in\mathrm{Irr}(G)}\sum_{\substack{\gamma_{\chi_1},\gamma'_{\chi_1},\dots,\gamma_{\chi_s},\gamma'_{\chi_s}\notin\mathbb{R}\\ \gamma_{\chi_j}\neq\gamma'_{\chi_j}}}\widehat{\Phi}\Big(\frac{U\sum_{j=1}^s(\gamma_{\chi_j}-\gamma'_{\chi_j})}{2\pi}\Big)\prod_{j=1}^s\Big(\widehat{\eta}\Big(\frac{\gamma_{\chi_j}}{2\pi}\Big)\widehat{\eta}\Big(\frac{\gamma'_{\chi_j}}{2\pi}\Big)\Big)\\
&\qquad\qquad+O\Big(\frac{(\kappa_\eta[K:\mathbb{Q}]\log(\mathrm{rd}_L+2)\lambda_1(G)^2)^{2s}}{U}\Big).
\end{aligned}$$

The claimed bound follows since by positivity of $\widehat{\Phi}$ and $\widehat{\eta}$ we may remove any number of terms in the summation. □

We now give a lower bound for $\mathbb{V}_{2,s}(L/K;\eta)$ by noting that we may discard any number of terms in its defining sum, since each summand is non-negative.

Lemma 2.4. *Let L/K be a Galois extension and assume AC and GRH. Let $\eta\in\mathcal{S}_\delta,\Phi\in\mathcal{U}$. Assume moreover that there exists a (necessarily real) character $\vartheta\in\mathrm{Irr}(G)$ such that $|G|-f(|G|)\le\vartheta(1)^2\le|G|-1$ where f is a function such that $1\le f(|G|)\le\frac{1}{4}|G|$. Then for $s\in\mathbb{N}$ we have the bound*

$$\mathbb{V}_{2,s}(L/K;\eta)\ge H_s\big(\alpha(|\widehat{\eta}|^2)[K:\mathbb{Q}]|G|^{\frac12}\log(\mathrm{rd}_L)\big)^s\Big(1+O\Big(\frac{sf(G)^{\frac12}}{|G|^{\frac12}}+\frac{s^2}{\log\log(\mathrm{rd}_L+2)}\Big)\Big),$$

where H_s is defined by (4).

Proof of Lemma 2.4. Firstly, for $s=1$ the claimed bound is trivial since $\mathbb{V}_{2,s}(L/K;\eta)=0$. For $s\ge 2$, restricting the sum in (9) to the character ϑ, we have the lower bound

$$\mathbb{V}_{2,s}(L/K;\eta)\ge V_s(\vartheta;\eta):=\sum_{\substack{\gamma_{1,1},\gamma_{1,2},\dots,\gamma_{s,1},\gamma_{s,2}\neq 0\\ \gamma_{j,1}\neq\gamma_{j,2}\\ \sum_{j=1}^s(\gamma_{j,1}-\gamma_{j,2})=0\\ \forall i\le s\,\forall k\in\{1,2\}\,\exists!\,j\neq i:\gamma_{i,k}\in\{-\gamma_{j,1},\gamma_{j,2}\}}}\prod_{j=1}^s\Big(\widehat{\eta}\Big(\frac{\gamma_{j,1}}{2\pi}\Big)\widehat{\eta}\Big(\frac{\gamma_{j,2}}{2\pi}\Big)\Big),\tag{11}$$

where the $\gamma_{j,k}$ run through the imaginary parts of the non-trivial zeros of $L(s,L/K,\vartheta)$. We define $\mathcal{H}_s$ to be the set of involutions $\pi:\{1,\dots,s\}\times\{1,2\}\to\{1,\dots,s\}\times\{1,2\}$ having no fixed point and such that $\pi(j,1)\neq(j,2)$ for all $j\le s$. We have $H_s=|\mathcal{H}_s|$. Given $\pi\in\mathcal{H}_s$, we define

$$\Gamma_\pi:=\left\{(\gamma_{1,1},\gamma_{1,2},\dots,\gamma_{s,1},\gamma_{s,2}):\ \begin{array}{l}\forall(j,k),\gamma_{j,k}\neq 0,\\ \forall(j,k),(i,\ell),(\gamma_{j,k}+(-1)^{\ell-k}\gamma_{i,\ell}=0)\Rightarrow(i,\ell)=\pi(j,k)\end{array}\right\}.$$

Now, given $\pi\in\mathcal{H}_s$, we note that the vector $(\gamma_{1,1},\gamma_{1,2},\dots,\gamma_{s,1},\gamma_{s,2})\in\Gamma_\pi$ where for all (j,k), $\gamma_{j,k}=\varepsilon_{j,k}\gamma_{\pi(j,k)}$ and where by definition $\varepsilon_{j,k}=-1$ if $\pi(j,k)_2=k$ and $\varepsilon_{j,k}=1$

otherwise, corresponds to a summand on the right hand side of (11). Note that if π_1, π_2 are distinct involutions, then the corresponding vectors of zeros are distinct. We deduce that

$$V_s(\vartheta;\eta) \geq \sum_{\pi\in H_s} \sum_{\substack{(\gamma_{1,1},\gamma_{1,2},\dots,\gamma_{s,1},\gamma_{s,2})\in\Gamma_\pi \\ \forall j,k,\gamma_{j,k}=\varepsilon_{j,k}\gamma_{\pi(j,k)}}} \prod_{j=1}^{s} \Big(\widehat{\eta}\Big(\frac{\gamma_{j,1}}{2\pi}\Big)\widehat{\eta}\Big(\frac{\gamma_{j,2}}{2\pi}\Big)\Big).$$

Reindexing, we see that the innermost sum is

$$\begin{aligned}
&\geq \sum_{\gamma_1} \sum_{\gamma_2\notin\{\gamma_1,-\gamma_1\}} \cdots \sum_{\gamma_s\notin\{\gamma_1,-\gamma_1,\dots,\gamma_{s-1},-\gamma_{s-1}\}} \prod_{j=1}^{s} \Big(m(\tfrac{1}{2}+i\gamma_j)\Big|\widehat{\eta}\Big(\frac{\gamma_j}{2\pi}\Big)\Big|^2\Big) \\
&\geq \sum_{\gamma_1} \sum_{\gamma_2\notin\{\gamma_1,-\gamma_1\}} \cdots \sum_{\gamma_s\notin\{\gamma_1,-\gamma_1,\dots,\gamma_{s-1},-\gamma_{s-1}\}} \prod_{j=1}^{s} \Big|\widehat{\eta}\Big(\frac{\gamma_j}{2\pi}\Big)\Big|^2 \\
&\geq b_0(\vartheta;|\widehat{\eta}|^2)^{s-2}\big(b_0(\vartheta;|\widehat{\eta}|^2)^2 + O(s^2 b_0^+(\vartheta;|\widehat{\eta}|^4))\big),
\end{aligned}$$

where the γ_j run through the imaginary parts of the non-trivial zeros of $L(s, L/K, \vartheta)$ and $m(\frac{1}{2}+i\gamma_j)$ denotes the multiplicity of the corresponding zero, and where

$$b_0(\chi;|\widehat{\eta}|^2) := \sum_{\rho_\chi\notin\mathbb{R}} \Big|\widehat{\eta}\Big(\frac{\rho_\chi-\frac{1}{2}}{2\pi i}\Big)\Big|^2, \qquad b_0^+(\chi;|\widehat{\eta}|^2) = \sum_{\rho_\chi\notin\mathbb{R}} m(\rho_\chi)\Big|\widehat{\eta}\Big(\frac{\rho_\chi-\frac{1}{2}}{2\pi i}\Big)\Big|^2.$$

By the bound [4, Theorem 5] on multiplicities of zeros, the total contribution of the error term is

$$\ll H_s s^2 \frac{(\log(A(\vartheta)))^s}{\log\log A(\vartheta)^{\frac{3}{\vartheta(1)}}} \ll H_s s^2 \frac{(\vartheta(1)[K:\mathbb{Q}]\log(\mathrm{rd}_L+2))^s}{\log\log(\mathrm{rd}_L+2)},$$

by Lemma 2.1. By the same bound on multiplicities, one can replace $b_0(\vartheta;|\widehat{\eta}|^2)$ with $b(\vartheta;|\widehat{\eta}|^2)$ at the cost of an error term which is also $\ll H_s s^2 \frac{(\vartheta(1)[K:\mathbb{Q}]\log(\mathrm{rd}_L+2))^s}{\log\log(\mathrm{rd}_L+2)}$. The proof is finished by applying [3, Lemma 4.2] as well as Lemma 2.2. □

We are now ready to prove Theorem 1.1.

Proof of Theorem 1.1. The proof is obtained by combining Lemmas 2.3 and 2.4. □

3. Groups having a unique character of large degree: Proof of Theorem 1.2

In this section we focus on a specific case of groups $G = \mathrm{Gal}(L/K)$ having a unique character of large degree. Our goal will be to establish a lower bound on the averaged moment $M_{n,1}(U; L/K, \Phi, \eta)$ (recall (6)) and prove Theorem 1.2, which will allow us to deduce non-Gaussian behaviour in families of such Galois extensions.

Let G be a non-trivial finite group and let χ be an irreducible representation of G of degree $d = \chi(1)$. It is a classical fact form the representation theory of finite groups over $\mathbb{C}$ that $d \mid |G|$ and $d^2 \leq |G|$. Therefore one may write $|G| = d(d+e)$ for some positive integer e. Note that if $e < d$ then necessarily G has a unique irreducible character of degree d.

In [9], Snyder classifies the groups for which $e = 1$ and shows that for fixed $e \geq 2$ there are only finitely many (with an explicit bound depending only on e) isomorphism classes of groups G such that $|G| = d(d+e)$. For $e = 1$, Snyder's result is the following (see [9, Prop. 2.1]).

Proposition 3.1 (Snyder)**.** *Let G be a finite group. The following assertions are equivalent.*

(1) *There exists $\chi \in \mathrm{Irr}(G)$ of degree d such that $d(d+1) = |G|$,*
(2) *Either $G \simeq \mathbb{Z}/2\mathbb{Z}$ or G is a doubly transitive Frobenius group i.e. it is isomorphic to the semi direct product of a subgroup N of order $d+1$ by a subgroup H of order d that acts freely and transitively by conjugation on $N \smallsetminus \{1\}$.*

Moreover if $|G| > 2$ the character χ in (1), which is necessarily unique, is induced from any non trivial character of degree 1 of the subgroup N of (2).

Remark. Slightly more generally, assume $|G| = d(d+e)$ where $d = \lfloor \sqrt{|G|} \rfloor > 1$ is the degree of some $\chi \in \mathrm{Irr}(G)$. Then the inequality $d(d+3) > (d+1)^2$ implies $e \in \{1, 2\}$. One deduces that G is either a doubly transitive Frobenius group, or an abelian group of order ≤ 3 or a non abelian group of order 8 (by Proposition 3.1 and [9, Th. 6.2]).

In the sequel we exclude the case $G \simeq \mathbb{Z}/2\mathbb{Z}$ (*i.e.* $d = 1$). In view of their importance in Proposition 3.1, we recall the definition of *Frobenius group* (see [7, Prop. 16.5]). Let G be a finite group having a normal subgroup N and a subgroup $H \notin \{\{1\}, G\}$ such that $G = NH$. The group G is a *Frobenius group of kernel N and complement H* if, for all $h \in H \smallsetminus \{1\}$, conjugation by h acts without fixed points on $N \smallsetminus \{1\}$. If in addition the action of H on $N \smallsetminus \{1\}$ is transitive, one says that G is a *doubly transitive* Frobenius group. The fact that this definition is equivalent to that of Proposition 3.1(2) is straightforward (indeed $N \cap H$ is trivial, from the fact that conjugation by any $h \in H$ is fixed point free on $N \smallsetminus \{1\}$). We next recall [7, Th. 18.7] which describes the representation theory of Frobenius groups.

Proposition 3.2. *Let G be a Frobenius group of kernel N and complement H. The group H acts on $\mathrm{Irr}(N)$ as follows*

$$\varphi^h := h \cdot \varphi \colon \big(x \mapsto \varphi(hxh^{-1})\big) \qquad (\varphi \in \mathrm{Irr}(N), h \in H)\,.$$

The orbits in this action are $\{\varphi_1 = 1_N\}$ as well as $\{\varphi^h \colon h \in H\}$ that has cardinality $|H|$ for any $\varphi \in \mathrm{Irr}(N) \smallsetminus \{1_N\}$. Let $\{\varphi_j \colon 2 \leq j \leq s\}$ be a system of representatives of the orbits in this action. A set of representatives for the isomorphism classes of the irreducible representations of G is given by

(1) *the irreducible representations of H via $G \to G/N \simeq H$,*
(2) *the induced representations $\mathrm{Ind}_N^G \varphi_j$, each of degree $|H|\varphi_j(1)$, for $2 \leq j \leq s$. These representations satisfy $N = \{x \in G \colon \mathrm{Tr}\big(\mathrm{Ind}_N^G \varphi_j(x)\big) \neq 0\}$.*

In particular G has $|\mathrm{Irr}(H)| + (|\mathrm{Irr}(N)| - 1)/|H|$ irreducible characters.

Corollary 3.3. *Let G be a doubly transitive Frobenius group of kernel N and complement H. Assume that H is abelian and non trivial. Then G has only one non abelian irreducible character: it is induced by any non trivial character of degree 1 of N. Moreover N is then necessarily abelian and $N \smallsetminus \{1\}$ is a conjugacy class of G.*

Proof. Let $d := |H| > 1$, hence $|G| = d(d+1)$ since $N \cap H$ is trivial and $N \smallsetminus \{1\}$ is a single orbit, with trivial stabilizer, under the action of H. We use the fact that H is abelian combined with Proposition 3.2 to deduce that

$$d(d+1) = |G| = \sum_{\chi \in \mathrm{Irr}(G)} \chi(1)^2 = |H| + \sum_{j=2}^{s} |H|^2 \varphi_j(1)^2 = d\Big(1 + d \sum_{j=2}^{s} \varphi_j(1)^2\Big)\,.$$

Therefore $s = 2$ and $\varphi_2(1) = 1$. By Proposition 3.2 this implies that G has a unique non abelian irreducible character defined by $\mathrm{Tr}\big(\mathrm{Ind}_N^G \varphi_2\big)$. Moreover $\mathrm{Irr}(N) \smallsetminus \{1_N\}$ is the orbit of the abelian character φ_2 under the action of H, hence N is abelian.

Finally since H acts transitively by conjugation on $N \smallsetminus \{1\}$ and since N is normal in G we deduce that $N \smallsetminus \{1\}$ is a conjugacy class of G. □

In [5, §9.2] and in [3, §2.2], a particular family of Galois extensions of $\mathbb{Q}$ having a doubly transitive Frobenius group as Galois group is considered. We recall its description in the example below.

Example 1. Let a, p be distinct prime numbers such that $p \neq 2$ and $a^{p-1} \not\equiv 1 \bmod p^2$ and let $K_{a,p}$ be the splitting field inside $\mathbb{C}$ of $X^p - a \in \mathbb{Q}[X]$. Then $G := \mathrm{Gal}(K_{a,p}/\mathbb{Q})$ is isomorphic to the group of transformations of the affine line $\mathbb{A}^1_{\mathbb{F}_p}$; it is a doubly transitive Frobenius group. Indeed G can be described as follows:

$$G \simeq \left\{ \begin{pmatrix} c & d \\ 0 & 1 \end{pmatrix} : c \in \mathbb{F}_p^*, d \in \mathbb{F}_p \right\} .$$

Here the Frobenius kernel N and the Frobenius complement H are respectively

$$N := \left\{ \begin{pmatrix} 1 & \star \\ 0 & 1 \end{pmatrix} \right\} , \qquad H = \left\{ \begin{pmatrix} \star & 0 \\ 0 & 1 \end{pmatrix} : \star \in \mathbb{F}_p^\times \right\} .$$

The group G admits p irreducible characters: $p-1$ of them are lifts of the characters of H *via* the isomorphism $G/N \simeq H$. The unique non abelian irreducible character of G has degree $p-1$ and is non zero only on two conjugacy classes: $\{1\}$ and $N \smallsetminus \{1\}$.

The last property mentioned in the example is more generally enjoyed by any doubly transitive Frobenius group G (as seen by combining Proposition 3.1 and Proposition 3.2(2)): the unique non abelian irreducible character of G vanishes on all but two conjugacy classes. This property, which has been studied by group theorists for independent reasons (see *e.g.* [6]), implies in our case a general form of orthogonality of characters, as we now show.

Proposition 3.4. *Let G be a doubly transitive Frobenius group of order $d(d+1) \geq 6$ with kernel N and abelian complement H of order d. Denote by $\{1 = \psi_1, \dots, \psi_d\}$ the irreducible characters of H, which all have degree 1 (by abuse of notation we will see these characters as characters of degree 1 of G). Finally denote by ϑ the unique non abelian character of G. It satisfies*

$$\vartheta(1) = d\,, \qquad \vartheta(N \smallsetminus \{1\}) = -1\,, \qquad \big(g \in G \smallsetminus N \Rightarrow \vartheta(g) = 0\big)\,.$$

In particular, for any $n \geq 1$ and any choice of irreducible characters $\chi_1, \dots, \chi_n$ (with possible repetitions) of G, one has the generalized orthogonality relations

$$\sum_{C \in G^\sharp} |C| \chi_1(C) \cdots \chi_n(C) = \begin{cases} |G| \delta(\chi_1 \cdots \chi_n = 1), & \text{if } \chi_i \neq \vartheta\,, \text{ for all } i\,, \\ d^k + (-1)^k d, & \text{if } \chi_i = \vartheta\,, \text{ for } k \geq 1 \text{ values of } i\,. \end{cases} \tag{12}$$

Proof. This is a consequence of Corollary 3.3 together with the fact that $\langle \vartheta; \vartheta \rangle_G = 1$ and the equality $\psi_j(N) = \{1\}$ which holds for all j. □

For a Galois extension of number fields L/K such that $G = \mathrm{Gal}(L/K)$ is a doubly transitive Frobenius group with a unique non abelian character ϑ, we will now bound $(-1)^n M_{n,1}(U; L/K, \Phi, \eta)$ in terms of the sums

$$S_{n,k}(L/K,\eta) := \sum_{\substack{\chi_1,\dots,\chi_{n-k}\in\mathrm{Irr}(G)\\ \forall i,\chi_i\neq\vartheta}} \sum_{\substack{\gamma_{\chi_1},\dots,\gamma_{\chi_{n-k}},\gamma_{\vartheta,1},\dots,\gamma_{\vartheta,k}\neq 0\\ \gamma_{\chi_1}+\cdots+\gamma_{\chi_{n-k}}+\gamma_{\vartheta,1}+\cdots+\gamma_{\vartheta,k}=0}} \prod_{i=1}^{n-k}\widehat{\eta}\Big(\frac{\gamma_{\chi_i}}{2\pi}\Big)\prod_{j=1}^{k}\widehat{\eta}\Big(\frac{\gamma_{\vartheta,j}}{2\pi}\Big) \qquad (k\le n-1);$$

$$S_{n,n}(L/K,\eta) := \sum_{\substack{\gamma_{\vartheta,1},\dots,\gamma_{\vartheta,n}\neq 0\\ \gamma_{\vartheta,1}+\cdots+\gamma_{\vartheta,n}=0}} \prod_{j=1}^{n}\widehat{\eta}\Big(\frac{\gamma_{\vartheta,j}}{2\pi}\Big).$$

Lemma 3.5. *Let G be a doubly transitive Frobenius group of order $d(d+1)\geq 6$ with kernel N and abelian complement H of order d. Let L/K be a Galois extension of number fields of group G, and assume GRH. Let $\eta\in\mathcal{S}_\delta$, $\Phi\in\mathcal{U}$. For $U\geq 1$, we have the following bound:*

$$(-1)^n M_{n,1}(U;L/K,\Phi,\eta) \geq \sum_{\substack{\chi_1,\dots,\chi_n\in\mathrm{Irr}(G)\\ \forall i,\chi_i\neq\vartheta\\ \chi_1\cdots\chi_n=1}} \sum_{\substack{\gamma_{\chi_1},\dots,\gamma_{\chi_n}\neq 0\\ \sum_{i=1}^n\gamma_{\chi_i}=0}} \prod_{i=1}^{n}\widehat{\eta}\Big(\frac{\gamma_{\chi_i}}{2\pi}\Big) + \sum_{k=1}^{n}\binom{n}{k}\frac{d^{k-1}+(-1)^k}{d+1}S_{n,k}(L/K,\eta) + O\big(U^{-1}(d+1)^{2n-2}([K:\mathbb{Q}]\log(\mathrm{rd}_L+2))^n\big), \tag{13}$$

where ϑ denotes the unique non-abelian character of G, and the $\gamma_{\vartheta,j}$ run through the imaginary parts of the non-trivial zeros of $L(s,L/K,\vartheta)$. In particular, since all summands in this expression are non-negative, it follows that for $n=2m$,

$$M_{2m,1}(U;L/K,\Phi,\eta) \geq \frac{d^{2m-1}+1}{d+1}S_{2m,2m}(L/K,\eta) + O\big(U^{-1}(d+1)^{4m-2}([K:\mathbb{Q}]\log(\mathrm{rd}_L+2))^{2m}\big). \tag{14}$$

Proof. Applying orthogonality of characters in the form

$$\psi_\eta(\mathrm{e}^u;L/K,1_C) = \frac{|C|}{|G|}\sum_{\chi\in\mathrm{Irr}(G)}\overline{\chi}(C)\psi_\eta(\mathrm{e}^u;L/K,\chi),$$

we obtain the expression

$$\begin{aligned}\mathcal{M}_n(u;L/K,\eta) &= \frac{1}{|G|}\sum_{C\in G^\sharp}|C|\Big(\frac{|G|}{|C|}\psi_\eta(\mathrm{e}^u;L/K,1_C) - \mathrm{e}^{\frac{u}{2}}\mathcal{L}_\eta(\tfrac12) - \widehat{\eta}(0)z(L/K,\tfrac{|G|}{|C|}1_C)\Big)^n\\ &= \frac{1}{|G|}\sum_{\chi_1,\dots,\chi_n\in\mathrm{Irr}(G)}\prod_{j=1}^{n}\psi_\eta^*(\mathrm{e}^u,L/K,\chi_j)\sum_{C\subset G^\sharp}|C|\overline{\chi_1}(C)\cdots\overline{\chi_n}(C),\end{aligned}$$

where

$$\psi_\eta^*(\mathrm{e}^u,L/K,\chi) := \psi_\eta(\mathrm{e}^u,L/K,\chi) - 1_{\chi=1}\mathrm{e}^{\frac{u}{2}}\mathcal{L}_\eta(\tfrac12) - \widehat{\eta}(0)z(L/K,\chi).$$

Combining this formula with Proposition 3.4, it follows that

$$\mathcal{M}_n(u; L/K, \eta) = \sum_{\substack{\chi_1,\dots,\chi_n \in \mathrm{Irr}(G) \\ \forall i, \chi_i \neq \vartheta \\ \chi_1 \cdots \chi_n = 1}} \prod_{j=1}^{n} \psi_\eta^*(\mathrm{e}^u, L/K, \chi_j)$$
$$+ \frac{1}{|G|} \sum_{k=1}^{n} \binom{n}{k} \psi_\eta^*(\mathrm{e}^u, L/K, \vartheta)^k \sum_{\substack{\chi_1,\dots,\chi_{n-k} \in \mathrm{Irr}(G) \\ \forall i, \chi_i \neq \vartheta}} \prod_{j=1}^{n-k} \psi_\eta^*(\mathrm{e}^u, L/K, \chi_j)\big(d^k + (-1)^k d\big)\,,$$

where by convention the innermost sum is equal to 1 when $k = n$. Hence,

$$(-1)^n M_{n,1}(U; L/K, \Phi, \eta) = M'_{n,1}(U; L/K, \Phi, \eta) + M''_{n,1}(U; L/K, \Phi, \eta), \tag{15}$$

where

$$M'_{n,1}(U; L/K, \Phi, \eta) := \frac{(-1)^n}{\int_0^\infty \Phi} \int_0^\infty \Phi(\tfrac{u}{U}) \sum_{\substack{\chi_1,\dots,\chi_n \in \mathrm{Irr}(G) \\ \forall i, \chi_i \neq \vartheta \\ \chi_1 \cdots \chi_n = 1}} \prod_{j=1}^{n} \psi_\eta^*(\mathrm{e}^u, L/K, \chi_j) \frac{\mathrm{d}u}{U},$$

$$M''_{n,1}(U; L/K, \Phi, \eta) := \frac{(-1)^n}{|G| \int_0^\infty \Phi} \sum_{k=1}^{n} \binom{n}{k} \big(d^k + (-1)^k d\big) \times$$
$$\int_0^\infty \Phi(\tfrac{u}{U}) \psi_\eta^*(\mathrm{e}^u, L/K, \vartheta)^k \sum_{\substack{\chi_1,\dots,\chi_{n-k} \in \mathrm{Irr}(G) \\ \forall i, \chi_i \neq \vartheta}} \prod_{j=1}^{n-k} \psi_\eta^*(\mathrm{e}^u, L/K, \chi_j) \frac{\mathrm{d}u}{U}.$$

We recall that [3, Lemma 4.1] implies the estimate

$$\psi_\eta^*(\mathrm{e}^u; L/K, \chi) = -\sum_{\gamma_\chi \neq 0} \mathrm{e}^{i\gamma_\chi u} \widehat{\eta}\Big(\frac{\gamma_\chi}{2\pi}\Big) + O\big(\mathrm{e}^{-\frac{u}{2}} \log(A(\chi) + 2)\big),$$

as well as the bound (see [3, Lemmas 3.1 and 4.2])

$$\psi_\eta^*(\mathrm{e}^u; L/K, \chi) \ll \log(A(\chi) + 2) \ll \chi(1)[K : \mathbb{Q}] \log(\mathrm{rd}_L + 2).$$

Applying these estimates, it follows that

$$M'_{n,1}(U; L/K, \Phi, \eta) = \frac{1}{|G| \int_0^\infty \Phi} \sum_{k=1}^{n} \binom{n}{k} (d^k + (-1)^k d) \int_0^\infty \Phi(\tfrac{u}{U}) \tag{16}$$
$$\sum_{\substack{\chi_1,\dots,\chi_{n-k} \in \mathrm{Irr}(G) \\ \forall i, \chi_i \neq \vartheta}} \sum_{\substack{\gamma_{\chi_1},\dots,\gamma_{\chi_{n-k}} \neq 0 \\ \gamma_{\vartheta,1},\dots,\gamma_{\vartheta,k} \neq 0}} \mathrm{e}^{i(\sum_{j=1}^{k} \gamma_{\vartheta,j} + \sum_{i=1}^{n-k} \gamma_{\chi_i})u} \prod_{i=1}^{n-k} \widehat{\eta}\Big(\frac{\gamma_{\chi_i}}{2\pi}\Big) \prod_{j=1}^{k} \widehat{\eta}\Big(\frac{\gamma_{\vartheta,j}}{2\pi}\Big) \frac{\mathrm{d}u}{U} + E,$$

where the error term E satisfies the bound

$$|M'_{n,1}(U;L/K,\Phi,\eta)|+|E| \ll U^{-1}([K:\mathbb{Q}]\log(\mathrm{rd}_L+2))^n \sum_{\substack{\chi_1,\dots,\chi_n\in\mathrm{Irr}(G)\\ \forall i,\chi_i\neq\vartheta\\ \chi_1\cdots\chi_n=1}} 1$$

$$+ (|G|U)^{-1}\sum_{k=1}^{n}\binom{n}{k} d^{2k}([K:\mathbb{Q}]\log(\mathrm{rd}_L+2))^n \sum_{\substack{\chi_1,\dots,\chi_{n-k}\in\mathrm{Irr}(G)\\ \forall i,\chi_i\neq\vartheta}} 1$$

$$\ll U^{-1}(d+1)^{2n-2}\big([K:\mathbb{Q}]\log(\mathrm{rd}_L+2)\big)^n.$$

We observe that, as $\Phi\in\mathcal{U}$, Φ is even and

$$\int_0^\infty \Phi\Big(\frac{u}{U}\Big)\mathrm{e}^{i\gamma u}\frac{\mathrm{d}u}{U} = \frac{1}{2}\widehat{\Phi}\Big(\frac{U\gamma}{2\pi}\Big).$$

Then, the main term in (16) is

$$\geq \frac{1}{2\int_0^\infty\Phi}\sum_{k=1}^{n}\binom{n}{k}\frac{d^{k-1}+(-1)^k}{d+1}$$

$$\sum_{\substack{\chi_1,\dots,\chi_{n-k}\in\mathrm{Irr}(G)\\ \forall i,\chi_i\neq\vartheta}}\ \sum_{\substack{\gamma_{\chi_1},\dots,\gamma_{\chi_{n-k}}\neq 0\\ \gamma_{\vartheta,1},\dots,\gamma_{\vartheta,k}\neq 0}} \widehat{\Phi}\Big(\frac{U}{2\pi}\Big(\sum_{j=1}^{k}\gamma_{\vartheta,j}+\sum_{i=1}^{n-k}\gamma_{\chi_i}\Big)\Big)\prod_{i=1}^{n-k}\widehat{\eta}\Big(\frac{\gamma_{\chi_i}}{2\pi}\Big)\prod_{j=1}^{k}\widehat{\eta}\Big(\frac{\gamma_{\vartheta,j}}{2\pi}\Big),$$

which by positivity of $\widehat{\Phi}$ is greater than or equal to the second term in (13). Arguing similarly for the first term on the right hand side of (15) yields the claimed estimate.

□

In the next step we will bound the quantity $S_{2m,2m}(L/K,\eta)$ which appears in (14) through a second application of positivity. The key idea which will guide us in this task is that we believe that in the case where $L/\mathbb{Q}$ is Galois, the multiset of imaginary parts of non-trivial zeros of $\prod_{\chi\in\mathrm{Irr}(\mathrm{Gal}(L/\mathbb{Q}))}L(s,L/\mathbb{Q},\chi)$ is linearly independent over the rationals; this is known as hypothesis LI. With this in mind, we will drop all the terms for which LI does not hold; in particular, we will only consider the case where n and k are even. In the case where $K\neq\mathbb{Q}$, we refer the reader to [5, Section 1.2] for possible counterexamples to LI.

Lemma 3.6. *Let G be a doubly transitive Frobenius group of order $d(d+1)\geq 6$ with kernel N and abelian complement H of order d. Let ϑ be the unique non-abelian irreducible character of G, let L/K be a Galois extension of number fields of group G, and assume GRH. Let $\eta\in\mathcal{S}_\delta$. If $m\in\mathbb{N}$, then we have the bound*

$$S_{2m,2m}(L/K,\eta)\geq \mu_{2m}b_0(\vartheta,\widehat{\eta}^2)^{m-1}\max\Big\{b_0(\vartheta,\widehat{\eta}^2)-2m!m(m-1)||\widehat{\eta}||_\infty^2,0\Big\}.$$

Proof. Using positivity, thanks to [3, Lemma 5.3], we have

$$\begin{aligned} S_{2m,2m}(L/K,\eta) &= \sum_{\substack{\gamma_{\vartheta,1},\dots,\gamma_{\vartheta,2m}\neq 0\\ \gamma_{\vartheta,1}+\cdots+\gamma_{\vartheta,2m}=0}} \prod_{j=1}^{2m} \widehat{\eta}\Big(\frac{\gamma_{\vartheta,j}}{2\pi}\Big) \\ &\geq \binom{2m}{m} \sum_{\substack{\gamma_{\vartheta,1},\dots,\gamma_{\vartheta,2m}\neq 0\\ \gamma_{\vartheta,j}>0\,(\forall j\leq m),\,\gamma_{\vartheta,j}<0\,(\forall j>m)\\ (\forall\gamma\in\mathbb{R})\ |\{j:\gamma_{\vartheta,j}=\gamma\}|=|\{j:\gamma_{\vartheta,j}=-\gamma\}|}} \prod_{j=1}^{2m} \widehat{\eta}\Big(\frac{\gamma_{\vartheta,j}}{2\pi}\Big) \\ &\geq \mu_{2m} b_0(\vartheta,\widehat{\eta}^2)^{m-1} \max\Big\{b_0(\vartheta,\widehat{\eta}^2) - 2m!m(m-1)||\widehat{\eta}||_\infty^2, 0\Big\}. \end{aligned}$$

□

To conclude the proof of Theorem 1.2, we will need the following bound.

Lemma 3.7. *Let G be a doubly transitive Frobenius group of order $d(d+1)\geq 6$ with kernel N and abelian complement H of order d. Let L/K be a Galois extension of number fields of group G. Then one has the following lower bound:*

$$\log A(\vartheta) \geq (d-1)[K:\mathbb{Q}]\log(\mathrm{rd}_L).$$

Proof. Define for any non zero class function $t\colon G\to\mathbb{C}$ (see [3, (10)]),

$$S_t = \frac{\max_{a\neq 1}\big|\sum_{\chi\in\mathrm{Irr}(G)}|\widehat{t}(\chi)|^2\chi(a)\big|}{\lambda_{1,2}(t)},$$

where $\lambda_{1,2}(t)=\sum_{\chi\in\mathrm{Irr}(G)}\chi(1)|\widehat{t}(\chi)|^2$. One has $S_\vartheta=\frac{1}{d}$ by the definition and properties of ϑ (see Proposition 3.4). The bound is then obtained by applying [3, Lemma 3.2]. □

We are now ready to prove Theorem 1.2.

Proof of Theorem 1.2. Combining Lemmas 3.5 and 3.6, we deduce that

$$\begin{aligned} M_{2m,1}(U;L/K,\Phi,\eta) \geq \frac{d^{2m-1}+1}{d+1}\mu_{2m} b_0(\vartheta,\widehat{\eta}^2)^{m-1}\max\Big\{b_0(\vartheta,\widehat{\eta}^2)-2m!m(m-1)||\widehat{\eta}||_\infty^2,0\Big\} \\ + O\big(U^{-1}(d+1)^{4m-2}([K:\mathbb{Q}]\log(\mathrm{rd}_L+2))^{2m}\big). \end{aligned}$$

Applying [3, Lemma 4.2] and [5, Lemma 4.1] to estimate $b_0(\vartheta,\widehat{\eta}^2)$, we see that the first term in this expression is

$$\begin{aligned} &\geq \frac{\mu_{2m}d^{2m}}{d(d+1)}\widehat{\eta}^{2m}(0)\Big(\log A(\vartheta)+O(d[K:\mathbb{Q}])\Big)^m \\ &\geq \frac{\mu_{2m}d^{2m}}{d(d+1)}\widehat{\eta}^{2m}(0)\Big((d-1)[K:\mathbb{Q}]\log(\mathrm{rd}_L)\Big)^m\Big(1+O\Big(\frac{m}{\log(\mathrm{rd}_L+2)}\Big)\Big), \end{aligned}$$

by Lemma 3.7. The first claimed result follows.

As for the second, note that in the limit as $U\to\infty$, the variance $M_{2,1}(U;L/K,\Phi,\eta)$ is asymptotically at most $d^2[K:\mathbb{Q}]^2\log(\mathrm{rd}_L)^2(1+o_{d\to\infty}(1))$ (combine (5) with [3, Lemma 4.1]). The claimed bound follows from combining this upper bound with the lower bound (7). □

Acknowledgements

The work of the third author was partly funded by the ANR through project FLAIR (ANR-17-CE40-0012). The authors would like to thank *Villa La Stella* in Florence for their hospitality and excellent working conditions during a stay in March 2022 where substantial parts of this work were accomplished.

References

[1] R. de la Bretèche and D. Fiorilli, *On a conjecture of Montgomery and Soundararajan*, Math. Annalen **381** (2021), no. 1, 575–591.

[2] ———, *Moments of moments of primes in arithmetic progressions* (2020), available at arXiv:2010.05944.

[3] R. de la Bretèche, D. Fiorilli, and F. Jouve, *Moments in the Chebotarev Density Theorem: general class functions* (2022).

[4] E. Carneiro, V. Chandee, and M. B. Milinovich, *A note on the zeros of zeta and L-functions*, Math. Z. **281** (2015), no. 1-2, 315–332.

[5] D. Fiorilli and F. Jouve, *Distribution of Frobenius elements in families of Galois extensions* (2020), available at hal-02464349.

[6] S. M. Gagola Jr., *Characters vanishing on all but two conjugacy classes*, Pacific J. Math. **109** (1983), no. 2, 363–385.

[7] B. Huppert, *Character theory of finite groups*, De Gruyter Expositions in Mathematics, vol. 25, Walter de Gruyter & Co., Berlin, 1998.

[8] H. Iwaniec and E. Kowalski, *Analytic number theory*, American Mathematical Society Colloquium Publications, vol. 53, American Mathematical Society, Providence, RI, 2004.

[9] N. Snyder, *Groups with a character of large degree*, Proc. Amer. Math. Soc. **136** (2008), no. 6, 1893–1903.

Université Paris Cité, Sorbonne Université, CNRS, Institut de Mathématiques de Jussieu-Paris Rive Gauche, F-75013 Paris, France
E-mail address: regis.delabreteche@imj-prg.fr

Univ. Paris-Saclay, CNRS, Laboratoire de mathématiques d'Orsay, 91405, Orsay, France.
E-mail address: daniel.fiorilli@universite-paris-saclay.fr

Univ. Bordeaux, CNRS, Bordeaux INP, IMB, UMR 5251, F-33400, Talence, France.
E-mail address: florent.jouve@math.u-bordeaux.fr