Algebra & Number Theory

Volume 13
2019
No. 10

msp

Algebra & Number Theory

msp.org/ant

See inside back cover or msp.org/ant for submission instructions.

The subscription price for 2019 is US $385/year for the electronic version, and $590/year (+$60, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscriber address should be sent to MSP.

Algebra & Number Theory (ISSN 1944-7833 electronic, 1937-0652 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

ANT peer review and production are managed by EditFLOW® from MSP.

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

http://msp.org/

ALGEBRA AND NUMBER THEORY 13:10 (2019)
dx.doi.org/10.2140/ant.2019.13.2243

The elliptic KZB connection and algebraic de Rham theory for unipotent fundamental groups of elliptic curves

Ma Luo

We develop an algebraic de Rham theory for unipotent fundamental groups of once punctured elliptic curves over a field of characteristic zero using the universal elliptic KZB connection of Calaque, Enriquez and Etingof (2009) and Levin and Racinet (2007). We use it to give an explicit version of Tannaka duality for unipotent connections over an elliptic curve with a regular singular point at the identity.

This paper is mostly written at Duke University, and then revised at University of Oxford.

MSC2010: primary 11G05; secondary 14F40, 32G34.
Keywords: elliptic KZB connection, unipotent fundamental groups, algebraic de Rham theory.

Introduction

A once punctured elliptic curve is an elliptic curve with its identity removed. In this paper, we describe an algebraic de Rham theory for unipotent fundamental groups of once punctured elliptic curves by explicit computations.

The analytic version of this story is described by Calaque, Enriquez and Etingof [Calaque et al. 2009] and by Levin and Racinet [2007]. For a family $\mathscr{X} \to T$ where each fiber X_t over $t \in T$ is a once punctured elliptic curve,

$$\begin{array}{ccc} X_t & \subset & \mathscr{X} \\ \Big| & & \Big| \\ t & \in & T \end{array}$$

there is a vector bundle $\mathcal{P}$ of prounipotent groups over $\mathscr{X}$, endowed with a flat connection. For a point $x \in \mathscr{X}$ that lies over t, i.e., $x \in X_t$, the fiber of $\mathcal{P}$ over x is the unipotent fundamental group $\pi_1^{\mathrm{un}}(X_t, x)$. We are particularly interested in the case when $\mathscr{X} = \mathcal{E}'$ and $T = \mathcal{M}_{1,1}$. In this case, the flat connection is called the universal elliptic KZB[1] connection.[2] The bundle $\mathcal{P}$ extends naturally by Deligne's canonical extension $\overline{\mathcal{P}}$ to $\overline{\mathcal{E}}$, and the universal elliptic KZB connection on $\overline{\mathcal{P}}$ has regular singularities around boundary divisors: the identity section of the universal elliptic curve $\mathcal{E} \to \mathcal{M}_{1,1}$ and the nodal cubic. One can restrict the bundle $\mathcal{P}$ to a single fiber of $\mathcal{E}' \to \mathcal{M}_{1,1}$, i.e., a once punctured elliptic curve $E' := E \setminus \{\mathrm{id}\}$, and obtain Deligne's canonical extension $\overline{\mathcal{P}}$ of it to E. It is endowed with a unipotent connection on E, having regular singularity at the identity. We call this the elliptic KZB connection on E.

Working algebraically, Levin and Racinet have shown that there is a $\mathbb{K}$-structure on the bundle $\mathcal{P}$ over a punctured elliptic curve X defined over a field $\mathbb{K}$ of characteristic zero, and a $\mathbb{Q}$-structure for the bundle $\mathcal{P}$ over $\mathcal{M}_{1,2/\mathbb{Q}}$. However, their algebraic formulas for the (universal) elliptic KZB connection is neither explicit nor having regular singularity at the identity (section). By resolving these issues for the case of $\mathcal{M}_{1,2}$, we will prove:

Theorem. *There is an explicit $\mathbb{Q}$-de Rham structure $\overline{\mathcal{P}}_{\mathrm{dR}}$ on the bundle $\overline{\mathcal{P}}$ over $\overline{\mathcal{M}}_{1,2}$ with the universal elliptic KZB connection, which has regular singularities along boundary divisors, the identity section and the nodal cubic.*

Restricting to a single elliptic curve, we get:

Corollary. *If E is an elliptic curve defined over a field $\mathbb{K}$ of characteristic zero, then there is an explicit $\mathbb{K}$-de Rham structure $\overline{\mathcal{P}}_{\mathrm{dR}}$ on the bundle $\overline{\mathcal{P}}$ over E with an elliptic KZB connection, which has regular singularity at the identity.*

[1] Named after physicists Knizhnik, Zamoldchikov and Bernard.

[2] The general universal elliptic KZB connection is the flat connection on the bundle $\mathcal{P}$ over $\mathcal{M}_{1,n+1}$ whose fiber over $[E; 0, x_1, \dots, x_n]$ is the unipotent fundamental group of the configuration space of n points on E' with base point $(x_1, \dots, x_n)$. Calaque et al. [2009] write down the universal elliptic KZB connection for all $n \geq 1$.

It is well known that these de Rham structures exist and can be constructed via Tannaka duality. But the explicit nature allows us to compute the image of these de Rham structures on the complexification of the Betti ones.

In the classical case of $\mathbb{P}^1 \setminus \{0, 1, \infty\}$, there is a trivial vector bundle $\mathcal{P}$ on it with fiber $\mathbb{C}\langle\langle \boldsymbol{e}_0, \boldsymbol{e}_1 \rangle\rangle$, formal power series in noncommuting generators $\boldsymbol{e}_0, \boldsymbol{e}_1$, and with the KZ connection

$$\nabla = d - \frac{dz}{z}\boldsymbol{e}_0 + \frac{dz}{1-z}\boldsymbol{e}_1,$$

where $\boldsymbol{e}_0, \boldsymbol{e}_1$ act on the fiber by left multiplication. This bundle extends via Deligne's canonical extension to a trivial bundle $\overline{\mathcal{P}}$ over $\mathbb{P}^1$ with the same connection having regular singularities at $0, 1, \infty$. One can view this bundle as a universal object of the tannakian category

$$\mathcal{C}_{\mathbb{Q}} := \left\{ \begin{array}{c} \text{unipotent vector bundles } \overline{\mathcal{V}} \text{ over } \mathbb{P}^1 \text{ defined over } \mathbb{Q} \text{ with a flat connection } \nabla \\ \text{that has regular singularities at } 0, 1, \infty \text{ with nilpotent residue} \end{array} \right\},$$

and interpret the KZ connection as a universal unipotent connection on $\mathbb{P}^1_{/\mathbb{Q}}$. Moreover, classical polylogarithms

$$\mathrm{Li}_k(z) := \sum_{n>0} \frac{z^n}{n^k}, \quad k \geq 1$$

and their generalizations

$$\mathrm{Li}_{k_1,\dots,k_r}(z) := \sum_{n_1 > \cdots > n_r > 0} \frac{z^{n_1}}{n_1^{k_1} \cdots n_r^{k_r}}, \quad r > 0, k_i > 0,$$

interpreted [Beilinson and Deligne 1994] as periods of unipotent variations of mixed Hodge structures on $\mathbb{P}^1 - \{0, 1, \infty\}$, can be expressed as (regularized) iterated integrals of algebraic 1-forms dz/z and $dz/(1-z)$ that appear in the KZ connection.

It is important to note from [Deligne 1989, Section 12] that in the "good" case when a smooth variety X is defined over a field $\mathbb{K}$, and its compactification $\overline{X}$ satisfies the conditions of

$$H^0(\overline{X}, \mathcal{O}) = \mathbb{K} \quad \text{and} \quad H^1(\overline{X}, \mathcal{O}) = 0,$$

Deligne's canonical extension to $\overline{X}$ of a unipotent vector bundle $\mathcal{V}$ over X, $\overline{\mathcal{V}}$, is a trivial bundle. Clearly this works for $X = \mathbb{P}^1 \setminus \{0, 1, \infty\}$, and allows one to define a *global fiber functor* on the tannakian category $\mathcal{C}_{\mathbb{Q}}$ of unipotent connections over $\mathbb{P}^1_{/\mathbb{Q}}$ with regular singularities at $0, 1, \infty$. However, this does not work for punctured elliptic curves.

The tricky part in our elliptic case is that Deligne's canonical extension of $\mathcal{P}_{\mathrm{dR}}$, $\overline{\mathcal{P}}_{\mathrm{dR}}$, is not a trivial bundle as the corresponding monodromy representation fails a Hodge theoretic restriction (see [Hain 1986]). We trivialize the bundle $\overline{\mathcal{P}}_{\mathrm{dR}}$ on two open subsets of the (universal) elliptic curve, and write down algebraic connection formulas according to these trivializations, with suitable gauge transformation on their intersection. These two opens are E' and E'' (correspondingly, $\mathcal{E}'$ and $\mathcal{E}''$ for the universal elliptic curve $\mathcal{E}$), where E'', containing the identity, is the complement of three nontrivial 2-torsion points of E (the trivial one being the identity).

For a single elliptic curve $E_{/\mathbb{K}}$, this bundle $\overline{\mathcal{P}}_{\mathrm{dR}}$ is a universal object of the tannakian category

$$\mathcal{C}_{\mathbb{K}}^{\mathrm{dR}} := \left\{ \begin{array}{c} \text{unipotent vector bundles } \overline{\mathcal{V}} \text{ over } E \text{ defined over } \mathbb{K} \text{ with a flat connection } \nabla \\ \text{that has regular singularity at the identity with nilpotent residue} \end{array} \right\}.$$

This allows us to compute the tannakian fundamental group $\pi_1(\mathcal{C}_{\mathbb{K}}^{\mathrm{dR}}, \omega)$ of this category, where the fiber functor ω is the fiber over a $\mathbb{K}$-rational point of E. It is a free pronilpotent group of rank 2 defined over $\mathbb{K}$. This tannakian formalism implies that the elliptic KZB connection that we have computed explicitly on the algebraic vector bundle $\overline{\mathcal{P}}_{\mathrm{dR}}$ can be viewed as a universal unipotent connection over $E_{/\mathbb{K}}$. Similar results have been recently obtained by Enriquez and Etingof [2018] for the configuration space of n points in an elliptic curve E with ground field $\mathbb{C}$.

The elliptic KZB connection enables us to construct closed[3] iterated integrals of algebraic 1-forms of any lengths on E, so that one can compute the (regularized) periods of $\pi_1^{\mathrm{un}}(E', \vec{\mathsf{v}})$, where $\vec{\mathsf{v}}$ is a tangential base point at the identity. This leads naturally to elliptic polylogarithms [Beilinson and Levin 1994; Brown and Levin 2011; Levin and Racinet 2007]. Note that it is not known in general how to construct closed iterated integrals of algebraic 1-forms of lengths 3 or more. In Section 7A, we show that the naive elliptic analogue of the KZ connection

$$\nabla = d - \frac{x\,dx}{y}\mathsf{T} + \frac{dx}{y}\mathsf{S},$$

which we call the naive connection, is somewhat different than the elliptic KZB connection, see Proposition 7.2 for the precise statement. However, one can show that the elliptic KZB connection on E is algebraically gauge equivalent to the naive connection up to degree 5, see Remark 7.3. Therefore, periods constructed from both connections, as iterated integrals of algebraic 1-forms of lengths at most 5, are the same.

Part I. Background

1. Moduli spaces of elliptic curves

Here we quickly review the construction of moduli spaces of elliptic curves and their Deligne–Mumford compactifications. Full details can be found in [Katz and Mazur 1985; Hain 2011], or the first section of [Hain 2013].

1A. ***Moduli spaces as algebraic stacks.*** Denote the moduli stack over $\mathbb{Q}$ of elliptic curves with n marked points and r nonzero tangent vectors by $\mathcal{M}_{1,n+\vec{r}}$. The Deligne–Mumford compactification of $\mathcal{M}_{1,n}$ will be denoted by $\overline{\mathcal{M}}_{1,n}$.

[3] i.e., homotopy invariant.

One can view $\mathcal{M}_{1,n+1}$ as the stack quotient of $\mathcal{M}_{1,n+\vec{1}}$ by the $\mathbb{G}_m$-action

$$\lambda : [E; x_1, \dots, x_n; \omega] \mapsto [E; x_1, \dots, x_n; \lambda\omega],$$

where a moduli point $[E; x_1, \dots, x_n; \omega] \in \mathcal{M}_{1,n+\vec{1}}$ is represented by tuples

$$(E; x_1, \dots, x_n; \omega),$$

an elliptic curve E with n marked points and the differential form ω that is dual to the marked tangent vector.

For example, the moduli space $\mathcal{M}_{1,\vec{1}}$ over $\mathbb{Q}$ can be described explicitly as the scheme

$$\mathcal{M}_{1,\vec{1}} = \mathbb{A}^2_{\mathbb{Q}} \setminus D,$$

where D is the discriminant locus $\{(u, v) \in \mathbb{A}^2 : \Delta = u^3 - 27v^2 = 0\}$, see [Katz and Mazur 1985, Section 2.2]. The point (u, v) corresponds to the once punctured elliptic curve (the plane cubic) $y^2 = 4x^3 - ux - v$ with the abelian differential dx/y. The moduli stack $\mathcal{M}_{1,1}$ can be defined as the quotient of $\mathcal{M}_{1,\vec{1}}$ by the $\mathbb{G}_m$-action

$$\lambda \cdot (u, v) = (\lambda^{-4}u, \lambda^{-6}v).$$

Its compactification, the moduli stack $\overline{\mathcal{M}}_{1,1}$, is the quotient of $Y := \mathbb{A}^2 - \{(0, 0)\}$[4] by the same $\mathbb{G}_m$-action above.

Similarly, define the moduli stack $\mathcal{M}_{1,2}$ over $\mathbb{Q}$ to be the quotient of the scheme

$$\mathcal{M}_{1,1+\vec{1}} := \{(x, y, u, v) \in \mathbb{A}^2 \times \mathbb{A}^2 : y^2 = 4x^3 - ux - v, \text{ and } u^3 - 27v^2 \neq 0\}$$

by the $\mathbb{G}_m$-action

$$\lambda : (x, y, u, v) \mapsto (\lambda^{-2}x, \lambda^{-3}y, \lambda^{-4}u, \lambda^{-6}v).$$

Here the point $(x, y, u, v) \in \mathcal{M}_{1,1+\vec{1}}$ corresponds to the point (x, y) on the punctured elliptic curve $y^2 = 4x^3 - ux - v$ with the abelian differential dx/y. Note that $\mathcal{M}_{1,2}$ is $\mathcal{E}'$, the universal elliptic curve $\mathcal{E}$ over $\mathcal{M}_{1,1}$ with its identity section removed. We define its compactification $\overline{\mathcal{M}}_{1,2}$ as the quotient of the scheme

$$\{(x, y, u, v) \in \mathbb{A}^2 \times \mathbb{A}^2 : y^2 = 4x^3 - ux - v, (u, v) \neq (0, 0)\}$$

by the same $\mathbb{G}_m$-action above. Note that $\overline{\mathcal{M}}_{1,2}$ is the compactification $\bar{\mathcal{E}}$ of the universal elliptic curve $\mathcal{E}$ whose restriction to the q-disk is the Tate curve $\mathcal{E}_{\text{Tate}} \to \operatorname{Spec} \mathbb{Z}[\![q]\!]$ (see [Silverman 1994, Chapter V]).

1B. ***Moduli spaces as complex analytic orbifolds.*** Working complex analytically, we can define moduli spaces as complex orbifolds

$$\mathcal{M}^{\text{an}}_{1,1} := \mathbb{G}_m \backslash\!\backslash \mathcal{M}^{\text{an}}_{1,\vec{1}}, \quad \mathcal{M}^{\text{an}}_{1,2} := \mathbb{G}_m \backslash\!\backslash \mathcal{M}^{\text{an}}_{1,1+\vec{1}},$$

where $\mathcal{M}^{\text{an}}_{1,\vec{1}} := \mathcal{M}_{1,\vec{1}}(\mathbb{C})$ and $\mathcal{M}^{\text{an}}_{1,1+\vec{1}} := \mathcal{M}_{1,1+\vec{1}}(\mathbb{C})$ are complex analytic manifolds.

[4]One may regard Y as a partial compactification of $\mathcal{M}_{1,\vec{1}}$.

The moduli space $\mathcal{M}_{1,1}^{\mathrm{an}}$ can also be defined as the orbifold quotient $\mathrm{SL}_2(\mathbb{Z})\backslash\backslash\mathfrak{h}$ of the upper half plane $\mathfrak{h}$ by the standard $\mathrm{SL}_2(\mathbb{Z})$ action

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} : \tau \mapsto \gamma\tau = \frac{a\tau + b}{c\tau + d}$$

where $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ and $\tau \in \mathfrak{h}$. The map

$$\begin{aligned} \mathfrak{h} &\to \mathcal{M}_{1,\vec{1}}^{\mathrm{an}} = \{(u, v) \in \mathbb{C}^2 : u^3 - 27v^2 \neq 0\} \\ \tau &\mapsto \left(20G_4(\tau), \tfrac{7}{3}G_6(\tau)\right) \end{aligned}$$

induces an isomorphism of orbifolds $\mathrm{SL}_2(\mathbb{Z})\backslash\backslash\mathfrak{h} \cong \mathbb{G}_m\backslash\backslash\mathcal{M}_{1,\vec{1}}^{\mathrm{an}}$, where $G_{2n}(\tau)$ is the normalized Eisenstein series of weight $2n$ (see Section 3A for a definition).

A point $\tau \in \mathfrak{h}$ corresponds to the framed elliptic curve $E_\tau := \mathbb{C}/\Lambda_\tau$ where $\Lambda_\tau := \mathbb{Z} \oplus \mathbb{Z}\tau$, with a basis $\boldsymbol{a}, \boldsymbol{b}$ of $H_1(E_\tau; \mathbb{Z})$ that corresponds to $1, \tau$ of the lattice Λ_τ via the identification $H_1(E_\tau; \mathbb{Z}) \cong \Lambda_\tau$.

There is a canonical family of elliptic curves $\mathcal{E}_{\mathfrak{h}}$ over the upper half plane $\mathfrak{h}$, called the universal framed family of elliptic curves in [Hain 2011], whose fiber over $\tau \in \mathfrak{h}$ is E_τ. It is the quotient of the trivial bundle $\mathbb{C} \times \mathfrak{h} \to \mathfrak{h}$ by the $\mathbb{Z}^2$-action:

$$(m, n) : (\xi, \tau) \mapsto \left(\xi + (m, n)\begin{pmatrix} \tau \\ 1 \end{pmatrix}, \tau\right).$$

The universal elliptic curve $\mathcal{E}^{\mathrm{an}}$ over $\mathcal{M}_{1,1}^{\mathrm{an}}$ is the orbifold quotient of $\mathbb{C} \times \mathfrak{h}$ by the semidirect product[5] $\mathrm{SL}_2(\mathbb{Z}) \ltimes \mathbb{Z}^2$, where $\mathbb{Z}^2$ acts on $\mathbb{C} \times \mathfrak{h}$ as above, and $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ acts as follows:

$$\gamma : (\xi, \tau) \mapsto ((c\tau + d)^{-1}\xi, \gamma\tau).$$

The universal elliptic curve $\mathcal{E}^{\mathrm{an}}$ can also be obtained as the orbifold quotient of $\mathcal{E}_{\mathfrak{h}} \to \mathfrak{h}$ by $\mathrm{SL}_2(\mathbb{Z})$. It is an orbifold family of elliptic curves whose fiber over a moduli point $[E] \in \mathcal{M}_{1,1}$ is an elliptic curve isomorphic to E. If we remove all the lattice points $\Lambda_{\mathfrak{h}} := \{(\xi, \tau) \in \mathbb{C} \times \mathfrak{h} : \xi \in \Lambda_\tau\}$ from $\mathbb{C} \times \mathfrak{h}$, then take the orbifold quotient of the same $\mathrm{SL}_2(\mathbb{Z}) \ltimes \mathbb{Z}^2$-action above, we obtain another analytic description of the moduli space $\mathcal{M}_{1,2}^{\mathrm{an}}$. To relate the two descriptions, there is a map

$$\begin{aligned} (\mathbb{C} \times \mathfrak{h}) - \Lambda_{\mathfrak{h}} &\to \mathcal{M}_{1,1+\vec{1}}^{\mathrm{an}} = \{(x, y, u, v) \in \mathbb{C}^2 \times \mathbb{C}^2 : y^2 = 4x^3 - ux - v, (u, v) \neq (0, 0)\} \\ (\xi, \tau) &\mapsto \left(P_2(\xi, \tau), -2P_3(\xi, \tau), 20G_4(\tau), \tfrac{7}{3}G_6(\tau)\right) \end{aligned}$$

that induces an isomorphism $\mathrm{SL}_2(\mathbb{Z}) \ltimes \mathbb{Z}^2\backslash\backslash((\mathbb{C} \times \mathfrak{h}) - \Lambda_{\mathfrak{h}}) \cong \mathbb{G}_m\backslash\backslash\mathcal{M}_{1,1+\vec{1}}^{\mathrm{an}}$, where $P_2(\xi, \tau)$ and $P_3(\xi, \tau)$ are, up to a constant, the Weierstrass $\wp$-function $\wp_\tau(\xi)$ and its derivative $\wp'_\tau(\xi)$ (see Section 3B for the definition).

[5]The semiproduct structure is induced from the right action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathbb{Z}^2$: $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) : (m\ n) \mapsto (m\ n)\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$.

2. The local system $\mathbb{H}$ with its Betti and $\mathbb{Q}$-de Rham realizations

The local system $\mathbb{H}$ over $\mathcal{M}_{1,1}$ is a "motivic local system", which has a set of compatible realizations: Betti, $\mathbb{Q}$-de Rham, Hodge and l-adic described in [Hain and Matsumoto 2018, Section 5]. In this section we will follow [loc. cit., Section 5] closely and describe its Betti realization $\mathbb{H}^{\mathrm{B}}$ and $\mathbb{Q}$-de Rham realization $\mathcal{H}^{\mathrm{dR}}$, and the comparison between these two.

We will denote the pullback of $\mathbb{H}$ (resp. $\mathbb{H}^{\mathrm{B}}$, $\mathcal{H}^{\mathrm{dR}}$) to $\mathcal{M}_{1,n+\vec{r}}$ by $\mathbb{H}_{n+\vec{r}}$ (resp. $\mathbb{H}^{\mathrm{B}}_{n+\vec{r}}$, $\mathcal{H}^{\mathrm{dR}}_{n+\vec{r}}$), so that $\mathbb{H}_1$ (resp. $\mathbb{H}^{\mathrm{B}}_1$, $\mathcal{H}^{\mathrm{dR}}_1$) is the same as $\mathbb{H}$ (resp. $\mathbb{H}^{\mathrm{B}}$, $\mathcal{H}^{\mathrm{dR}}$).

2A. *Betti realization* $\mathbb{H}^{\mathbf{B}}$. The Betti realization $\mathbb{H}^{\mathrm{B}}$ is the local system $R^1\pi_*^{\mathrm{an}}\mathbb{Q}$ over $\mathcal{M}_{1,1}^{\mathrm{an}}$ associated to the universal elliptic curve $\pi^{\mathrm{an}} : \mathcal{E}^{\mathrm{an}} \to \mathcal{M}_{1,1}^{\mathrm{an}}$. We identify it, via Poincaré duality $H^1(E) \to H_1(E)$ fiberwise, with the local system over $\mathcal{M}_{1,1}^{\mathrm{an}}$ whose fiber over $[E] \in \mathcal{M}_{1,1}$ is $H_1(E;\mathbb{Q})$.

There is a natural $\mathrm{SL}_2(\mathbb{Z})$ action

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} : \begin{pmatrix} \boldsymbol{b} \\ \boldsymbol{a} \end{pmatrix} \mapsto \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \boldsymbol{b} \\ \boldsymbol{a} \end{pmatrix},$$

where $\boldsymbol{a}, \boldsymbol{b}$ is the basis of $H_1(E_\tau;\mathbb{Z})$ that corresponds to the basis $1, \tau$ of Λ_τ. The sections $\boldsymbol{a}, \boldsymbol{b}$ trivialize the pullback $\mathbb{H}_{\mathfrak{h}}$ of $\mathbb{H}^{\mathrm{B}}$ to $\mathfrak{h}$.

Denote the dual basis of $H^1(E_\tau;\mathbb{Q}) \cong \mathrm{Hom}(H_1(E_\tau),\mathbb{Q})$ by $\check{\boldsymbol{a}}, \check{\boldsymbol{b}}$. Then, under Poincaré duality,

$$\check{\boldsymbol{a}} = -\boldsymbol{b} \text{ and } \check{\boldsymbol{b}} = \boldsymbol{a}.$$

And the corresponding $\mathrm{SL}_2(\mathbb{Z})$ action on this dual basis is

$$\gamma : \begin{pmatrix} \boldsymbol{a} & -\boldsymbol{b} \end{pmatrix} \mapsto \begin{pmatrix} \boldsymbol{a} & -\boldsymbol{b} \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

One can construct the local system $\mathbb{H}^{\mathrm{B}}$ by taking the orbifold quotient of the local system $\mathbb{H}_{\mathfrak{h}} \to \mathfrak{h}$ by the above $\mathrm{SL}_2(\mathbb{Z})$-action.

2B. $\mathbb{Q}$*-de Rham realization* $\mathcal{H}^{\mathbf{dR}}$. The $\mathbb{Q}$-de Rham realization $\mathcal{H}^{\mathrm{dR}}$ is an algebraic vector bundle $H^1(\mathcal{E}/\mathcal{M}_{1,1})$ over $\mathbb{Q}$, defined by relative cohomology, on $\mathcal{M}_{1,1/\mathbb{Q}}$ equipped with the Gauss–Manin connection. By our definition $\mathcal{M}_{1,1} := \mathbb{G}_m \backslash\backslash \mathcal{M}_{1,\vec{1}}$, to work with $\mathcal{M}_{1,1}$ is to work $\mathbb{G}_m$-equivariantly with $\mathcal{M}_{1,\vec{1}}$. We first construct the corresponding algebraic vector bundle on $\mathcal{M}_{1,\vec{1}}$. Define a vector bundle

$$\mathcal{H}^{\mathrm{dR}}_{\vec{1}} := \mathcal{O}_{\mathcal{M}_{1,\vec{1}}}\mathsf{S} \oplus \mathcal{O}_{\mathcal{M}_{1,\vec{1}}}\mathsf{T}$$

over $\mathcal{M}_{1,\vec{1}}$ with a $\mathbb{G}_m$-action:

$$\lambda \cdot \mathsf{S} = \lambda^{-1}\mathsf{S} \quad \text{and} \quad \lambda \cdot \mathsf{T} = \lambda \mathsf{T},$$

where the sections S and T represent algebraic differential forms $x\,dx/y$ and dx/y respectively. This $\mathbb{G}_m$-action extends the action on $\mathcal{M}_{1,\vec{1}}$ to the bundle $\mathcal{H}^{\mathrm{dR}}_{\vec{1}}$ over it.

The Gauss–Manin connection is explicitly given by

$$\nabla_0 = d + \left(-\frac{1}{12}\frac{d\Delta}{\Delta}\mathsf{T} + \frac{3\alpha}{2\Delta}\mathsf{S}\right)\frac{\partial}{\partial \mathsf{T}} + \left(-\frac{u\alpha}{8\Delta}\mathsf{T} + \frac{1}{12}\frac{d\Delta}{\Delta}\mathsf{S}\right)\frac{\partial}{\partial \mathsf{S}}, \tag{1}$$

where $\alpha = 2udv - 3vdu$, $\Delta = u^3 - 27v^2$ and $\partial/\partial\mathsf{S}$, $\partial/\partial\mathsf{T}$ a dual basis for S,T (see [Hain 2013, Proposition 19.6]). This connection is $\mathbb{G}_m$-invariant, and defined over $\mathbb{Q}$. Therefore, the bundle $\mathcal{H}^{\mathrm{dR}}_{\vec{1}}$ with connection ∇_0 over $\mathcal{M}_{1,\vec{1}}$ descends to a bundle $\mathcal{H}^{\mathrm{dR}}$ over $\mathcal{M}_{1,1}$.

The canonical extension $\overline{\mathcal{H}}^{\mathrm{dR}}_{\vec{1}}$ of $\mathcal{H}^{\mathrm{dR}}_{\vec{1}}$ to $Y := \mathbb{A}^2_{\mathbb{Q}} \setminus \{(0,0)\}$ is a vector bundle

$$\overline{\mathcal{H}}^{\mathrm{dR}}_{\vec{1}} := \mathcal{O}_Y\mathsf{S} \oplus \mathcal{O}_Y\mathsf{T}$$

with the same connection ∇_0 above. Since the connection has regular singularities along the discriminant locus $D = \{\Delta = 0\}$, and recall that $\overline{\mathcal{M}}_{1,1} = \mathbb{G}_m \backslash\!\backslash Y$ from Section 1A, the bundle $\overline{\mathcal{H}}^{\mathrm{dR}}_{\vec{1}} \to Y$ descends to a bundle $\overline{\mathcal{H}}^{\mathrm{dR}}$ over $\overline{\mathcal{M}}_{1,1}$ with regular singularity and nilpotent residue at the cusp. It is an extension of $\mathcal{H}^{\mathrm{dR}}$ over $\mathcal{M}_{1,1}$ to $\overline{\mathcal{M}}_{1,1}$.

2C. *The flat vector bundle $\mathcal{H}^{\mathrm{an}}$ and the comparison between $\mathcal{H}^{\mathrm{an}}$ and $\mathcal{H}^{\mathrm{dR}}$.* Define the holomorphic vector bundle

$$\mathcal{H}^{\mathrm{an}} := \mathbb{H}^{\mathrm{B}} \otimes \mathcal{O}_{\mathcal{M}^{\mathrm{an}}_{1,1}}$$

over $\mathcal{M}^{\mathrm{an}}_{1,1}$. The pullback of $\mathcal{H}^{\mathrm{an}}$ to $\mathfrak{h}$ (using the quotient map $\mathfrak{h} \to \mathcal{M}^{\mathrm{an}}_{1,1} = \mathrm{SL}_2(\mathbb{Z})\backslash\!\backslash\mathfrak{h}$) is the vector bundle

$$\mathcal{H}^{\mathrm{an}}_{\mathfrak{h}} = \mathcal{O}_{\mathfrak{h}}\boldsymbol{a} \oplus \mathcal{O}_{\mathfrak{h}}\boldsymbol{b},$$

where the sections $\boldsymbol{a}$ and $\boldsymbol{b}$ are flat.

Define a holomorphic section $\boldsymbol{w}$ of $\mathcal{H}^{\mathrm{an}}_{\mathfrak{h}}$ by

$$\boldsymbol{w}(\tau) = w_\tau = 2\pi i(\check{\boldsymbol{a}} + \tau\check{\boldsymbol{b}}) = 2\pi i(\tau\boldsymbol{a} - \boldsymbol{b}),$$

where w_τ is the class in $H^1(E_\tau;\mathbb{C})$ represented by the holomorphic differential $2\pi i\, d\xi$.

The sections $\boldsymbol{a}$ and $\boldsymbol{w}$ trivialize the pullback

$$\mathcal{H}^{\mathrm{an}}_{\mathbb{D}^*} := \mathcal{O}_{\mathbb{D}^*}\boldsymbol{a} \oplus \mathcal{O}_{\mathbb{D}^*}\boldsymbol{w}$$

of $\mathcal{H}^{\mathrm{an}}$ to $\mathbb{D}^*$ via the map

$$\mathfrak{h} \to \mathbb{D}^*, \quad \tau \mapsto q := e^{2\pi i\tau},$$

as they are invariant under $\gamma : \tau \mapsto \tau + 1$ $\big($with γ being $\pm\left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right)\big)$, and thus invariant under the monodromy action on the punctured q-disk $\mathbb{D}^*$.

An easy computation [Hain and Matsumoto 2018, Section 5.2] shows that the connection on $\mathcal{H}^{\mathrm{an}}_{\mathbb{D}^*}$ in terms of this framing is

$$\nabla^{\mathrm{an}}_0 = d + \boldsymbol{a}\frac{\partial}{\partial\boldsymbol{w}}\frac{dq}{q}.$$

Since this connection has a regular singularity at the cusp $q = 0$, we can extend $\mathcal{H}^{\mathrm{an}}_{\mathbb{D}^*}$ to the q-disk $\mathbb{D}$ by defining

$$\mathcal{H}^{\mathrm{an}}_{\mathbb{D}} := \mathcal{O}_{\mathbb{D}}\boldsymbol{a} \oplus \mathcal{O}_{\mathbb{D}}\boldsymbol{w}.$$

Therefore, we obtain Deligne's canonical extension $\overline{\mathcal{H}}^{\mathrm{an}}$ of $\mathcal{H}^{\mathrm{an}}$ to $\overline{\mathcal{M}}^{\mathrm{an}}_{1,1}$, endowed with a connection ∇^{an}_0 that has a regular singularity at the cusp.

To relate Betti and de Rham sections of $\mathcal{H}^{\mathrm{an}}$, we pull back the bundle $\mathcal{H}^{\mathrm{an}}_{\vec{1}}$ to $\mathfrak{h}$ via the map $\mathfrak{h} \to \mathcal{M}^{\mathrm{an}}_{1,\vec{1}}$ in Section 1B, and compare it with $\mathcal{H}^{\mathrm{an}}_{\mathfrak{h}}$.

Proposition 2.1. *There is a natural isomorphism*

$$(\overline{\mathcal{H}}^{\mathrm{an}}, \nabla^{\mathrm{an}}_0) \cong (\overline{\mathcal{H}}^{\mathrm{dR}}, \nabla_0) \otimes_{\mathcal{O}_{\overline{\mathcal{M}}_{1,1/\mathbb{Q}}}} \mathcal{O}_{\overline{\mathcal{M}}^{\mathrm{an}}_{1,1}}$$

induced from the pullback. The sections T *and* S *that correspond to* dx/y *and* $x\,dx/y$ *respectively, after being pulled back, become*

$$\mathsf{T} = \frac{\boldsymbol{w}}{2\pi i} \quad \textit{and} \quad \mathsf{S} = \frac{\boldsymbol{a} - 2G_2(\tau)\boldsymbol{w}}{2\pi i}.$$

Remark 2.2. Our formulas for T and S differ from those in Proposition 5.2 of [Hain and Matsumoto 2018] by a factor of $2\pi i$. The reason is that the cup product of dx/y and $x\,dx/y$ is $2\pi i$, and we have multiplied their Poincaré duals by $(2\pi i)^{-1}$ to obtain a $\mathbb{Q}$-de Rham basis of the first homology [Hain 2013, Section 20], such that $\mathsf{T} = \check{\mathsf{S}}$ and $\mathsf{S} = -\check{\mathsf{T}}$. More explanations are provided in Section 2D below.

2D. *The fiber of* $\mathbb{H}$ *at the cusp.* To better understand various Betti and de Rham sections of $\mathcal{H}^{\mathrm{an}}$, we observe the fiber $H := H_{\partial/\partial q}$ at the cusp associated to the tangent vector $\partial/\partial q$. One can compute the limit mixed Hodge structure on H (computed in [Hain and Matsumoto 2018, Section 5.4]), which is isomorphic to $\mathbb{Q}(0) \oplus \mathbb{Q}(-1)$, with Betti realization $H^{\mathrm{B}} = \mathbb{Q}\boldsymbol{a} \oplus \mathbb{Q}\boldsymbol{b}$, and de Rham realization $H^{\mathrm{dR}} = \mathbb{Q}\boldsymbol{a} \oplus \mathbb{Q}\boldsymbol{w}$. Note that on H, $-\boldsymbol{b} = \check{\boldsymbol{a}} = \boldsymbol{w}/2\pi i$ spans $\mathbb{Q}(-1)$ and $\boldsymbol{a} = \check{\boldsymbol{b}}$ spans $\mathbb{Q}(0)$.

One can think of H as the cohomology $H^1(E_{\partial/\partial q})$. It is better to work with first homology, which is the abelian quotient of the fundamental group. We use Poincaré duality to identify $H_1(E)$ with $H^1(E)(1)$. Therefore, we have $H_1(E_{\partial/\partial q}) = H(1) = \mathbb{Q}(1) \oplus \mathbb{Q}(0)$, with Betti realization $\mathbb{Q}\boldsymbol{a} \oplus \mathbb{Q}\boldsymbol{b}$ and de Rham realization $\mathbb{Q}\mathsf{A} \oplus \mathbb{Q}\mathsf{T}$, where

$$\mathsf{A} := \frac{\boldsymbol{a}}{2\pi i} \quad \text{and} \quad \mathsf{T} := \frac{\boldsymbol{w}}{2\pi i}.$$

Note that on $H(1)$, $\boldsymbol{a} = 2\pi i\mathsf{A}$ spans $\mathbb{Q}(1)$ and $-\boldsymbol{b} = \mathsf{T}$ spans $\mathbb{Q}(0)$.

By Proposition 2.1, we can write S in terms of this de Rham framing A, T of $\mathbb{H}$ (or in fact $\mathbb{H}(1)$)

$$\mathsf{S} = \mathsf{A} - 2G_2(\tau)\mathsf{T}.$$

We will use these sections A, S and T to write down the universal elliptic KZB connection in later sections.

3. Eisenstein elliptic functions and the Jacobi form $F(\xi, \eta, \tau)$

3A. *Eisenstein series.* A modular form[6] of weight k is a holomorphic function $f(\tau)$ on the upper half plane $\mathfrak{h}$ that satisfies

$$f(\gamma\tau) = (c\tau+d)^k f(\tau), \quad \text{where } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}),\ \tau \in \mathfrak{h}, \text{ and } \gamma\tau = \frac{a\tau+b}{c\tau+d},$$

and it extends to a holomorphic function on the q-disk.

Since $f(\tau+1) = f(\tau)$, it has a Fourier expansion of the form

$$f(\tau) = \sum_{n\in\mathbb{Z}} a_n q^n \quad \text{where } q = e^{2\pi i\tau}.$$

Since a modular form is holomorphic at the cusp, this q-series starts with terms of nonnegative q powers. Moreover, a modular form is called a cusp form if the leading coefficient a_0 of its q-series is 0.

Example 3.1 (weight k Eisenstein Series e_k). For integer $k > 0$, $\tau \in \mathfrak{h}$, define

$$e_k(\tau) := \sum_{\substack{n,m \\ (n,m)\neq(0,0)}} (n\tau+m)^{-k}.$$

Note that $e_k = 0$ if k is odd. For $k \geq 4$, the series for e_k is absolutely convergent. For $k = 2$, it has to be summed in a certain way, called *Eisenstein summation* [Weil 1976, Chapter III].

Example 3.2 (normalized Weight k Eisenstein Series G_k). We will normalize the Eisenstein series following Zagier [1991]. Define G_k to be zero when k is odd. For $k \geq 1$, define

$$G_{2k}(\tau) := \frac{1}{2}\frac{(2k-1)!}{(2\pi i)^{2k}} e_{2k}(\tau).$$

It has Fourier expansion

$$G_{2k}(\tau) = -\frac{B_{2k}}{4k} + \sum_{n=1}^{\infty} \sigma_{2k-1}(n) q^n$$

where the B_k are Bernoulli numbers[7] and $\sigma_k(n) = \sum_{d|n} d^k$, with

$$G_{2k}|_{q=0} = -\frac{B_{2k}}{4k} = \frac{(2k-1)!}{(2\pi i)^{2k}}\zeta(2k).$$

When $k > 2$ is even, G_k is holomorphic on the upper half plane, satisfying $G_k(\gamma\tau) = (c\tau+d)^k G_k(\tau)$, and it is holomorphic at the cusp. Therefore, it is a modular form of weight k. When $k = 2$, we have that G_2 satisfies (see [Zagier 1991])

$$G_2(\gamma\tau) = (c\tau+d)^2 G_2(\tau) + \frac{ic(c\tau+d)}{4\pi}.$$

It is well known that the ring of all modular forms is the polynomial ring $\mathbb{Q}[G_4, G_6]$.

[6] We will only consider modular forms of level one, i.e., those with respect to the entire modular group $\mathrm{SL}_2(\mathbb{Z})$.

[7] One can define Bernoulli numbers B_n by $x/(e^x-1) = \sum_{n=0}^{\infty} B_n x^n/n!$. Note that $B_0 = 1$, $B_1 = -\frac{1}{2}$ and that $B_{2k+1} = 0$ when $k > 0$.

3B. ***Eisenstein elliptic functions.*** For $k > 0$, $\tau \in \mathfrak{h}$ and $\xi \in \mathbb{C}$, define Eisenstein elliptic functions [Weil 1976] by

$$E_k(\xi, \tau) := \sum_{n,m} (\xi + n\tau + m)^{-k}.$$

Note that E_k is absolutely convergent for $k \geq 3$. For $k = 1, 2$, E_k is summed by *Eisenstein summation* [loc. cit., Chapter III]. We will need the following formula, which is adapted from (9) of Chapter IV in [loc. cit.].

Formula 3.3.

$$2\pi i \frac{\partial E_1}{\partial \tau} = E_3 - E_1 E_2.$$

Now we define functions $P_k(\xi, \tau)$ for $k \geq 2$:

$$P_k(\xi, \tau) := (2\pi i)^{-k}(E_k(\xi, \tau) - e_k(\tau)).$$

Note that up to a scalar, P_2 and P_3 are the Weierstrass $\wp$-function $\wp_\tau(\xi)$ and its derivative respectively.

These P_k satisfy recurrence relations [Weil 1976]: for $m \geq 3$, $n \geq 3$,

$$P_m P_n - P_{m+n} = \frac{(-1)^n}{(n-1)!} \sum_{h=1}^{m-2} \frac{2}{h!} G_{n+h} P_{m-h} + \frac{(-1)^m}{(m-1)!} \sum_{k=1}^{n-2} \frac{2}{k!} G_{m+k} P_{n-k} + (-1)^m \frac{2(m+n)}{m!n!} G_{m+n}$$

The same relation also holds for $m = 2$, $n \geq 2$.

By these relations, we know that the algebra generated by Eisenstein elliptic functions is the ring $\mathbb{K}[P_2, P_3]$ with coefficients in $\mathbb{K} := \mathbb{Q}[G_4, G_6]$.

Remark 3.4. If variable τ is fixed, one can use P_2, P_3 to embed the elliptic curve E_τ into a cubic in $\mathbb{P}^2$ (see Section 6), then P_k's are algebraic functions on this elliptic curve. In particular, if the elliptic curve E_τ is defined over a field $\mathbb{K}$ of characteristic 0, then there is an embedding with $G_4, G_6 \in \mathbb{K}$, so that $G_k \in \mathbb{K}$ for all $k \geq 4$. Therefore, P_k's are polynomials of P_2, P_3 with coefficients in $\mathbb{K}$, i.e., P_k's are in the coordinate ring $\mathcal{O}(E_{\tau/\mathbb{K}})$, which is a $\mathbb{K}$-algebra generated by P_2, P_3.

3C. ***The Jacobi forms $F(\xi, \eta, \tau)$ and $F^{\mathrm{Zag}}(u, v, \tau)$.*** There are two different versions of the Jacobi form F: one $F(\xi, \eta, \tau)$ used by Levin and Racinet [2007] and another $F^{\mathrm{Zag}}(u, v, \tau)$ used by Zagier [1991]. They are related to each other by

$$F(\xi, \eta, \tau) = 2\pi i F^{\mathrm{Zag}}(2\pi i\xi, 2\pi i\eta, \tau).$$

In this paper, we will use F^{Zag} exclusively. We list some properties of F^{Zag} here and leave the most relevant ones to the next subsection. These properties all follow from the theorem in [Zagier 1991, Section 3].

Proposition 3.5. *The function $F^{\mathrm{Zag}}(u, v, \tau)$ has the following properties*:

(1) $F^{\mathrm{Zag}}(u, v, \tau) = F^{\mathrm{Zag}}(v, u, \tau)$.

(2) $F^{\mathrm{Zag}}(u + 2\pi i, v, \tau) = F^{\mathrm{Zag}}(u, v, \tau)$.

(3) $F^{\mathrm{Zag}}(u + 2\pi i\tau, v, \tau) = \exp(-v) F^{\mathrm{Zag}}(u, v, \tau)$.

(4) $F^{\mathrm{Zag}}(u/(c\tau + d), v/(c\tau + d), \gamma\tau) = (c\tau + d)\exp(cuv/(2\pi i(c\tau + d))) F^{\mathrm{Zag}}(u, v, \tau)$, *where* $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ *and* $\gamma\tau = (a\tau + b)/(c\tau + d)$.

3D. ***Some useful formulas.*** In this section, we provide some formulas that will be used in later sections.

First, we express the Jacobi form F^{Zag} in terms of Eisenstein elliptic functions $P_k = (2\pi i)^{-k}(E_k - e_k)$ for $k \geq 2$ and $(2\pi i)^{-1}(E_1 - e_1) = (2\pi i)^{-1}E_1$. This is well-known, stated as Proposition-Definition(4.iii) in [Brown and Levin 2011, Section 3.4], also stated as (13) in [Levin and Racinet 2007] but with a typo.[8]

Formula 3.6.
$$T F^{\mathrm{Zag}}(2\pi i\xi, T, \tau) = \exp\left(-\sum_{k=1}^{\infty}\frac{(-T)^k}{k}P_k(\xi,\tau)\right).$$

Proof. By [Zagier 1991, page 456, (viii)]
$$F^{\mathrm{Zag}}(u, v, \tau) = \frac{u+v}{uv}\exp\left(\sum_{k>0}\frac{2}{k!}[u^k + v^k - (u+v)^k]G_k(\tau)\right).$$

Multiplying by v, then take logarithm on both sides, we get
$$\begin{aligned}\log(vF^{\mathrm{Zag}}(u, v, \tau)) &= \log\left(1+\frac{v}{u}\right) + \sum_{k>0}\frac{2}{k!}[u^k + v^k - (u+v)^k]G_k(\tau)\\ &= -\sum_{k=1}^{\infty}\frac{(-v/u)^k}{k} + \sum_{k=1}^{\infty}\frac{2v^k}{k!}\left[1+\left(\frac{u}{v}\right)^k - \left(1+\frac{u}{v}\right)^k\right]G_k(\tau)\end{aligned}$$

Let $u = 2\pi i\xi$, $v = T$, and rescale G_k back to e_k, we have
$$\begin{aligned}\log(TF^{\mathrm{Zag}}(2\pi i\xi, T, \tau)) &= -\sum_{k=1}^{\infty}\frac{(-T/2\pi i\xi)^k}{k} + \sum_{k=1}^{\infty}\frac{2T^k}{k!}\left[1+\left(\frac{2\pi i\xi}{T}\right)^k - \left(1+\frac{2\pi i\xi}{T}\right)^k\right]\frac{1}{2}\frac{(k-1)!}{(2\pi i)^k}e_k(\tau)\\ &= -\sum_{k=1}^{\infty}\frac{(-T)^k}{k}(2\pi i\xi)^{-k} - \sum_{l=1}^{\infty}\frac{T^l}{l}(2\pi i)^{-l}\sum_{k=1}^{l-1}\binom{l}{k}\left(\frac{2\pi i\xi}{T}\right)^{l-k}e_l(\tau)\\ &= -\sum_{k=1}^{\infty}\frac{(-T)^k}{k}(2\pi i)^{-k}\frac{1}{\xi^k} - \sum_{k=1}^{\infty}\frac{T^k}{k}(2\pi i)^{-k}\sum_{l=k+1}^{\infty}\frac{k}{l}\binom{l}{k}\xi^{l-k}e_l(\tau)\\ &= -\sum_{k=1}^{\infty}\frac{(-T)^k}{k}(2\pi i)^{-k}\frac{1}{\xi^k} - \sum_{k=1}^{\infty}\frac{(-T)^k}{k}(2\pi i)^{-k}(-1)^k\sum_{l=k+1}^{\infty}\binom{l-1}{k-1}\xi^{l-k}e_l(\tau)\\ &= -\sum_{k=1}^{\infty}\frac{(-T)^k}{k}(2\pi i)^{-k}\left[\frac{1}{\xi^k} + (-1)^k\sum_{l=k+1}^{\infty}\binom{l-1}{k-1}\xi^{l-k}e_l(\tau)\right]\\ &= -\sum_{k=1}^{\infty}\frac{(-T)^k}{k}(2\pi i)^{-k}(E_k - e_k)\\ &= -\sum_{k=1}^{\infty}\frac{(-T)^k}{k}P_k(\xi,\tau)\end{aligned}$$

[8] Equation (13) in [Levin and Racinet 2007] is missing a ξ on the left-hand side.

where the last line follows from (10) of Chapter III in [Weil 1976], and the facts that $\binom{l-1}{k-1} = 0$ for $l < k$ and that $e_k(\tau) = 0$ for odd k. After taking exponential on both sides, Formula 3.6 follows. $\square$

Taking partial derivative with respect to T, we have

Formula 3.7. $$T\frac{\partial F^{\mathrm{Zag}}}{\partial T}(2\pi i\xi, T, \tau) = \exp\biggl(-\sum_{k=1}^{\infty}\frac{(-T)^k}{k}P_k(\xi,\tau)\biggr)\biggl(\sum_{k=1}^{\infty}(-T)^{k-1}P_k(\xi,\tau) - \frac{1}{T}\biggr).$$

4. Unipotent completion of a group and its Lie algebra

Suppose we are given a finitely generated group Γ, and a field $\mathbb{K}$ of characteristic 0. The group algebra $\mathbb{K}\Gamma$ is naturally a Hopf algebra with coproduct, antipode and augmentation given by

$$\Delta : g \mapsto g \otimes g, \quad i : g \mapsto g^{-1}, \quad \epsilon : g \mapsto 1.$$

Note that it is cocommutative but not necessarily commutative, and thus does not correspond to the coordinate ring of a (pro-)algebraic group. It is natural to consider its (continuous) dual, which is commutative. We define the unipotent completion Γ^{un} of Γ over $\mathbb{K}$, a (pro-)algebraic group, by its coordinate ring

$$\mathcal{O}(\Gamma^{\mathrm{un}}_{/\mathbb{K}}) = \mathrm{Hom}_{\mathrm{cts}}(\mathbb{K}\Gamma, \mathbb{K}) := \varinjlim_n \mathrm{Hom}(\mathbb{K}\Gamma/I^n, \mathbb{K}),$$

where we give $\mathbb{K}\Gamma$ a topology by powers of its augmentation ideal $I := \ker\epsilon$. The set of its $\mathbb{K}$-rational points $\Gamma^{\mathrm{un}}(\mathbb{K})$ is in one-to-one correspondence with the set of

$$\{\text{ring homomorphisms } \mathcal{O}(\Gamma^{\mathrm{un}}_{/\mathbb{K}}) \to \mathbb{K}\}.$$

For example, any $\gamma \in \Gamma$ gives a ring homomorphism $\mathcal{O}(\Gamma^{\mathrm{un}}_{/\mathbb{K}}) \to \mathbb{K}$ by evaluating $\mathcal{O}(\Gamma^{\mathrm{un}}_{/\mathbb{K}})$ at γ, thus determines a $\mathbb{K}$-point $\gamma \in \Gamma^{\mathrm{un}}(\mathbb{K})$.

For the purpose of this paper, we only need to consider the case of Γ being a free group.

4A. ***The unipotent completion of a free group.*** Suppose that Γ is the free group $\langle x_1, \dots, x_n\rangle$ generated by the set $\{x_1, \dots, x_n\}$. The coordinate ring $\mathcal{O}(\Gamma^{\mathrm{un}})$ of its unipotent completion Γ^{un} over $\mathbb{K}$ is a $\mathbb{K}$ vector space spanned by a basis $\{a_I\}$ indexed by tuples $I = (i_1, i_2, \dots, i_r)$, where $i_j \in \{1, 2, \dots, n\}$. If the index is empty, then $a_\varnothing \equiv 1$; if the index tuple only consists of one number $I = (i)$, we will simply write a_I as a_i. The product structure on $\mathcal{O}(\Gamma^{\mathrm{un}})$ is induced by shuffle product Ш and linearity

$$a_I \cdot a_J = \sum_{K \in I Ш J} a_K.$$

For each $\mathbb{K}$-point $\gamma \in \Gamma^{\mathrm{un}}(\mathbb{K})$, "coordinate function" a_I takes value $a_I(\gamma)$ in $\mathbb{K}$, and

$$a_I(\gamma) \cdot a_J(\gamma) = \sum_{K \in I Ш J} a_K(\gamma). \tag{2}$$

Note that it is natural to define $\{a_1, \dots, a_n\}$ as the dual basis of $\{x_1, \dots, x_n\}$, so that $a_i(x_j) = \delta_{ij}$.

To determine the structure of Γ^{un}, consider the ring $\mathbb{K}\langle\langle X_1, \dots, X_n\rangle\rangle$ of formal power series in the noncommuting indeterminants X_j. It is a Hopf algebra with each X_j being primitive, and its augmentation ideal is the maximal ideal $I = (X_1, \dots, X_n)$.

There is a unique group homomorphism

$$\begin{aligned} \theta : \Gamma &\to \mathbb{K}\langle\langle X_1, \dots, X_n\rangle\rangle \\ \gamma &\mapsto \sum_I a_I(\gamma) X_I \end{aligned}$$

that takes x_j to $\exp(X_j)$, where for $I = (i_1, i_2, \dots, i_r)$, define $X_I := X_{i_1} X_{i_2} \cdots X_{i_r}$.

For any $\mathbb{K}$-point $\gamma \in \Gamma^{\mathrm{un}}(\mathbb{K})$, the element $\sum_I a_I(\gamma) X_I$ is group-like by (2). This induces a continuous isomorphism

$$\hat{\theta} : \Gamma^{\mathrm{un}}(\mathbb{K}) \to \{\text{group-like elements in } \mathbb{K}\langle\langle X_1, \dots, X_n\rangle\rangle^\wedge\},$$

where $\mathbb{K}\langle\langle X_1, \dots, X_n\rangle\rangle^\wedge$ is completed from $\mathbb{K}\langle\langle X_1, \dots, X_n\rangle\rangle$ with respect to its augmentation ideal.

It is easy to use universal mapping properties to prove:

Proposition 4.1. *The homomorphism $\hat{\theta}$ is an isomorphism of complete Hopf algebras.* □

Corollary 4.2. *The restriction of $\hat{\theta}$ induces a natural isomorphism*

$$d\hat{\theta} : \mathrm{Lie}(\Gamma^{\mathrm{un}}(\mathbb{K})) \to \mathbb{L}_{\mathbb{K}}(X_1, \dots, X_n)^\wedge$$

of topological Lie algebras.

Proof. This follows immediately from the fact that $\hat{\theta}$ induces an isomorphism on primitive elements and the well known fact that the set of primitive elements of the power series algebra $\mathbb{K}\langle\langle X_1, \dots, X_n\rangle\rangle$ is the completed free Lie algebra $\mathbb{L}_{\mathbb{K}}(X_1, \dots, X_n)^\wedge$. □

Remark 4.3. By the Baker–Campbell–Hausdorff formula, the exponential map

$$\exp : \mathbb{L}_{\mathbb{K}}(X_1, \dots, X_n)^\wedge \to \{\text{group-like elements in } \mathbb{K}\langle\langle X_1, \dots, X_n\rangle\rangle^\wedge\},$$

is a group isomorphism. Therefore, $\Gamma^{\mathrm{un}}(\mathbb{K})$ and its Lie algebra $\mathrm{Lie}(\Gamma^{\mathrm{un}}(\mathbb{K}))$ are isomorphic as groups.

5. Universal elliptic KZB connection — analytic formula

In this section, we describe the main object to be studied in this paper, working complex analytically. There is a canonical vector bundle $\mathcal{P}$ (resp. $\mathfrak{p}$) over $\mathcal{M}_{1,2}$ whose fiber over a moduli point $[E', x]$ is the unipotent fundamental group $\pi_1^{\mathrm{un}}(E', x)$ (resp. $\mathrm{Lie}(\pi_1^{\mathrm{un}}(E', x))$).[9] This vector bundle comes with an integrable connection, which is called the universal elliptic KZB connection. Analytic formulas for this connection have been given in different forms by Levin and Racinet [2007] and by Calaque, Enriquez and Etingof [2009].

[9] From Remark 4.3, the unipotent completion of a group and its Lie algebra are isomorphic, we will regard this bundle as a local system of both unipotent fundamental groups and Lie algebras, whichever is appropriate.

The universal elliptic KZB connection for the bundle $\mathcal{P}$ over $\mathcal{E}'$ actually lives on $\mathcal{E}$, even $\bar{\mathcal{E}}$. Since $\mathcal{P}$ over $\mathcal{E}'$ is a unipotent vector bundle, using Deligne's canonical extension, we obtain $\bar{\mathcal{P}}$ over $\bar{\mathcal{E}}$ by extending $\mathcal{P}$ across the boundary divisors, the identity section and the nodal cubic. The universal elliptic KZB connection has regular singularities around these divisors, as is shown in [Hain 2013, Sections 12 and 13].

By Section 4A, the fiber of $\mathcal{P}$ over a point $[E', x]$ is the Lie algebra $\mathrm{Lie}(\pi_1^{\mathrm{un}}(E', x))$ of its unipotent fundamental group $\pi_1^{\mathrm{un}}(E', x)$, which can be identified with $\mathbb{L}_{\mathbb{C}}(\mathsf{A}, \mathsf{T})^\wedge$, where A and T are the sections of $\mathbb{H}$ defined in Section 2D. Note that these sections, when pulled back to $\mathfrak{h}$, trivialize the vector bundle $\mathbb{H}_{\mathfrak{h}}$, with a factor of automorphy.[10] This factor of automorphy lifts to a general one on the bundle $\mathcal{P}$ over $\mathbb{C} \times \mathfrak{h}$.[11]

We now write the connection form in terms of analytic coordinates (ξ, τ) on $\mathbb{C} \times \mathfrak{h}$. It is shown to be $\mathrm{SL}_2(\mathbb{Z}) \ltimes \mathbb{Z}^2$-invariant in terms of the factor of automorphy we just described and flat in [Hain 2013, Section 9]. Therefore, it descends to a flat connection on the bundle $\mathcal{P}$ over the orbifold $\mathcal{E}$.

The connection is defined by

$$\nabla^{\mathrm{an}} f = df + \omega f,$$

with a 1-form

$$\omega \in \Omega^1((\mathbb{C} \times \mathfrak{h}) \log \Lambda_{\mathfrak{h}}) \otimes \mathrm{Der}\, \mathbb{L}_{\mathbb{C}}(\mathsf{A}, \mathsf{T})^\wedge,$$

whose analytic formula is given by

$$\omega = 2\pi i\, d\tau \otimes \mathsf{A}\frac{\partial}{\partial \mathsf{T}} + \psi + \nu,$$

with

$$\psi = \sum_{m \geq 1} \left(\frac{G_{2m+2}(\tau)}{(2m)!} 2\pi i\, d\tau \otimes \sum_{\substack{j+k=2m+1 \\ j,k>0}} (-1)^j [\mathrm{ad}_{\mathsf{T}}^j(\mathsf{A}), \mathrm{ad}_{\mathsf{T}}^k(\mathsf{A})] \frac{\partial}{\partial \mathsf{A}} \right),$$

and

$$\nu = \nu_1 + \nu_2 = \mathsf{T} F^{\mathrm{Zag}}(2\pi i \xi, \mathsf{T}, \tau) \cdot \mathsf{A} \otimes 2\pi i\, d\xi + \left(\frac{1}{\mathsf{T}} + \mathsf{T} \frac{\partial F^{\mathrm{Zag}}}{\partial \mathsf{T}}(2\pi i \xi, \mathsf{T}, \tau) \right) \cdot \mathsf{A} \otimes 2\pi i\, d\tau.$$

Here, we view $\mathbb{L}_{\mathbb{C}}(\mathsf{A}, \mathsf{T})^\wedge$ as a Lie subalgebra of $\mathrm{Der}\, \mathbb{L}_{\mathbb{C}}(\mathsf{A}, \mathsf{T})^\wedge$ via the adjoint action, and T^n denotes the n-time adjoint action $\mathrm{ad}_{\mathsf{T}}^n$ on $\mathbb{L}_{\mathbb{C}}(\mathsf{A}, \mathsf{T})^\wedge$; since every derivation $\delta \in \mathrm{Der}\, \mathbb{L}_{\mathbb{C}}(\mathsf{A}, \mathsf{T})^\wedge$ is determined by its values on A and T, it can be written uniquely in the form

$$\delta = \delta(\mathsf{A}) \frac{\partial}{\partial \mathsf{A}} + \delta(\mathsf{T}) \frac{\partial}{\partial \mathsf{T}}.$$

[10] The factor of automorphy on $\mathbb{H}_{\mathfrak{h}}$ is easily computed to be $M_\gamma(\tau) = \begin{pmatrix} (c\tau+d)^{-1} & 0 \\ c & c\tau+d \end{pmatrix}$ for $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$, cf. [Hain 2013, Example 3.4].

[11] The general factor of automorphy on $\mathcal{P}$ is

$$\widetilde{M}_\gamma(\xi, \tau) = \begin{cases} M_\gamma(\tau) \circ \exp(c\xi \mathsf{T}/(2\pi i(c\tau+d))) & \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \\ \exp(-m\mathsf{T}) & (m, n) \in \mathbb{Z}^2 \end{cases}$$

[Hain 2013, Section 6, (6.2)].

Part II. KZB Connection on a single elliptic curve

In this part, we describe an algebraic de Rham structure $\overline{\mathcal{P}}_{\mathrm{dR}}$ on the restriction of the canonical bundle $\overline{\mathcal{P}}$ to a single elliptic curve E. We essentially reproduce and then complete the unfinished work of Levin and Racinet [2007, Section 5]. In particular, their connection, though being algebraic, has an irregular singularity at the identity of the elliptic curve. Moreover, their formula is not explicit.

We compute explicitly the restriction of the universal elliptic KZB connection to a single elliptic curve in terms of its algebraic coordinates. We resolve the issue of irregular singularities at the identity in the connection formula by trivializing the bundle $\overline{\mathcal{P}}_{\mathrm{dR}}$ on two open subsets of E, one of which contains a neighborhood of the identity where the connection has a regular singularity. Therefore, we have constructed a de Rham structure $\overline{\mathcal{P}}_{\mathrm{dR}}$ on $\overline{\mathcal{P}}$ over E. Trivializing it on different open subsets is necessary because Deligne's canonical extension $\overline{\mathcal{P}}$ of $\mathcal{P}$ from E' (elliptic curve E punctured at the identity) to E, unlike the genus zero case (of $\mathbb{P}^1$), is not trivial as an algebraic vector bundle.

6. Elliptic curves as algebraic curves

Fix $\tau \in \mathfrak{h}$ and an elliptic curve $E = E_\tau$. Using the Weierstrass $\wp$-function

$$\wp_\tau(\xi) := E_2(\xi, \tau) - e_2(\tau),$$

we can embed a punctured elliptic curve E' into $\mathbb{P}^2$ as follows:

$$\xi \mapsto [(2\pi i)^{-2}\wp_\tau(\xi), (2\pi i)^{-3}\wp_\tau'(\xi), 1].$$ [12]

This satisfies an affine equation

$$y^2 = 4x^3 - ux - v,$$

where $u = g_2(\tau) = 20G_4(\tau)$, $v = g_3(\tau) = \frac{7}{3}G_6(\tau)$. It is defined over $\mathbb{K} := \mathbb{Q}(u, v)$. The identity of E is at the infinity. The equation $y = 0$ picks out three nontrivial order 2 elements in E (the trivial one being the identity), we define

$$E'' := E - \{y = 0\}.$$

Note that id $\in E''$, and $\{E', E''\}$ form an open cover of E.

By pulling back through the above embedding, one can identify algebraic functions and forms with their analytic counterparts, which is how we will turn the analytic formula of the connection into an algebraic formula. For example, coordinate functions x, $-y/2$ pull back to P_2, P_3 defined in Section 3B, and the differential dx/y pulls back to $2\pi i\, d\xi$. Note from Remark 3.4 that for $k \geq 2$, P_k can be expressed by a polynomial of P_2, P_3, i.e., $P_k = P_k(x, y) \in \mathbb{K}[x, y]$.

[12] We choose this embedding so that powers of $2\pi i$ will not appear in our algebra formulas of KZB connections later.

7. Algebraic connection formula over E'

Fix $\tau \in \mathfrak{h}$, an elliptic curve $E = E_\tau$ defined over a field $\mathbb{K}$ of characteristic zero, and its algebraic embedding as in the last section. The elliptic KZB connection restricted from the universal one to the once punctured elliptic curve $E' = E \setminus \{\mathrm{id}\}$ is

$$\nabla^{\mathrm{an}} = d + \nu_1 = d + \mathsf{T} F^{\mathrm{Zag}}(2\pi i\xi, \mathsf{T}, \tau) \cdot \mathsf{A} \otimes 2\pi i\, d\xi. \tag{3}$$

Note that when described in terms of sections A and T, the bundle $\mathcal{P}$ has factors of automorphy [Hain 2013, Section6]. We would like to make sections of $\mathcal{P}$ elliptic (i.e., periodic with respect to the lattice Λ_τ) by a gauge transformation so that the factor of automorphy is absorbed into it and become trivial. The connection form would also be elliptic and can be expressed in terms of algebraic coordinate functions x, y, and P_k's. Following Levin and Racinet [2007, Section 5] and using Formula 3.6, the connection transforms under the gauge $g_{\mathrm{alg}}(\xi) = \exp\bigl(-\frac{1}{2\pi i} E_1 \mathsf{T}\bigr)$ into $\nabla = d + \nu_1^{\mathrm{alg}}$, with 1-form

$$\begin{aligned}
\nu_1^{\mathrm{alg}} &= -dg_{\mathrm{alg}} \cdot g_{\mathrm{alg}}^{-1} + g_{\mathrm{alg}} \nu_1 g_{\mathrm{alg}}^{-1} \\
&= -\frac{1}{2\pi i} E_2 \mathsf{T}\, d\xi + \exp\Bigl(-\frac{E_1}{2\pi i}\mathsf{T}\Bigr) \exp\Bigl(-\sum_{k=1}^{\infty} \frac{(-\mathsf{T})^k}{k} P_k(\xi,\tau)\Bigr) \cdot \mathsf{A} \otimes 2\pi i\, d\xi \\
&= -(2\pi i)^{-2}(E_2 - e_2)\mathsf{T} \otimes 2\pi i d\xi + \exp\Bigl(-\sum_{k=2}^{\infty} \frac{(-\mathsf{T})^k}{k} P_k(\xi,\tau)\Bigr) \cdot (\mathsf{A} - (2\pi i)^{-2} e_2 \mathsf{T}) \otimes 2\pi i\, d\xi \\
&= -\frac{x\,dx}{y}\mathsf{T} + \exp\Bigl(-\sum_{k=2}^{\infty} \frac{(-\mathsf{T})^k}{k} P_k(x,y)\Bigr) \cdot \mathsf{S} \otimes 2\pi i\, d\xi \\
&= -\frac{x\,dx}{y}\mathsf{T} + \frac{dx}{y}\mathsf{S} + \sum_{n=2}^{\infty} q_n(x,y) \frac{dx}{y} \mathsf{T}^n \cdot \mathsf{S}.
\end{aligned}$$

Here $\nu_1^{\mathrm{alg}} \in \Omega^1(E'_{/\mathbb{K}}) \otimes \mathbb{L}_{\mathbb{K}}(\mathsf{S},\mathsf{T})^\wedge$, T^n is the action $\mathrm{ad}_{\mathsf{T}}^n$ on $\mathbb{L}_{\mathbb{K}}(\mathsf{S},\mathsf{T})^\wedge$ that repeats the adjoint action of T for n times, and

$$q_n(x,y) = \sum_{2a_2+3a_3+\cdots+na_n=n} \frac{1}{a_2!a_3!\cdots a_n!} \prod_{k=2}^{n} \Bigl(\frac{(-1)^{k+1} P_k(x,y)}{k}\Bigr)^{a_k} \in \mathcal{O}(E'_{/\mathbb{K}}),$$

where $\mathcal{O}(E'_{/\mathbb{K}}) = \mathbb{K}[x,y]/(y^2 - 4x^3 + ux + v)$. Note that the above sum is indexed by the partitions of integer n with summands at least 2. For example, 5 has 2 such partitions: 5 and $2+3$, so $q_5 = \frac{P_5}{5} + \bigl(-\frac{P_2}{2}\bigr) \cdot \frac{P_3}{3} = \frac{1}{5}P_5 - \frac{1}{6}P_2P_3$. Written as polynomials in $\mathbb{K}[x,y]$, we have $q_2 = -\frac{P_2}{2} = -\frac{1}{2}x$, $q_3 = \frac{P_3}{3} = -\frac{1}{6}y$, and $q_4 = \bigl(-\frac{P_4}{4}\bigr) + \frac{1}{2}\bigl(-\frac{P_2}{2}\bigr)^2 = \frac{u}{40} - \frac{x^2}{8}$.

Remark 7.1. One can use the recurrence relations of the P_k described in Section 3B to find relations among the q_n.

Note that the form ν_1^{alg} is defined over $\mathbb{K}$, so we have constructed an algebraic vector bundle $(\mathcal{P}_{\mathrm{dR}}, \nabla)$ over E' whose fibers can be identified with $\mathbb{L}_{\mathbb{K}}(\mathsf{S},\mathsf{T})^\wedge$. This algebraic bundle is defined over $\mathbb{K}$, with its connection ∇ also defined over $\mathbb{K}$. It provides us with a $\mathbb{K}$-structure $\mathcal{P}_{\mathrm{dR}}$ on $\mathcal{P}$ over E'. Since the form ν_1^{alg} has irregular singularity (xdx/y having a double pole) at the identity, we cannot extend it naively across the identity to obtain Deligne's canonical extension. To construct the canonical extension, we have to change gauge on a Zariski open neighborhood E'' of the identity. We do this in Section 8.

7A. ***The naive connection versus the elliptic KZB connection.*** Before we do this, we consider the naive connection on the trivial bundle

$$\mathbb{L}_{\mathbb{K}}(\mathsf{S},\mathsf{T})^\wedge \times E' \to E'$$

which is defined by $\nabla' = d + \nu_1^{\mathrm{naive}}$, where

$$\nu_1^{\mathrm{naive}} = -\frac{xdx}{y}\mathsf{T} + \frac{dx}{y}\mathsf{S}.$$ [13]

This flat connection is defined over $\mathbb{K}$, whose monodromy is a homomorphism $\rho^{\mathrm{naive}} : \pi_1(E', x) \to \mathbb{L}(\mathsf{S},\mathsf{T})^\wedge$ that induces an isomorphism

$$I^{\mathrm{naive}} : \operatorname{Lie} \pi_1^{\mathrm{un}}(E', x) \to \mathbb{L}(\mathsf{S},\mathsf{T})^\wedge.$$

Since the elliptic KZB connection $\nabla = d + \nu_1^{\mathrm{alg}}$ agrees with the naive connection up to degree 2, its monodromy $\rho^{\mathrm{KZB}} : \pi_1(E', x) \to \mathbb{L}(\mathsf{S},\mathsf{T})^\wedge$ also induces an isomorphism

$$I^{\mathrm{KZB}} : \operatorname{Lie} \pi_1^{\mathrm{un}}(E', x) \to \mathbb{L}(\mathsf{S},\mathsf{T})^\wedge.$$

Although both I^{naive} and I^{KZB} are isomorphisms of prounipotent groups, they can not be algebraically transferred from one to the other while preserving the group structure on $\mathbb{L}(\mathsf{S},\mathsf{T})^\wedge$.

Proposition 7.2. *Fix a field $\mathbb{K}$ of characteristic zero. Between the elliptic KZB connection $\nabla = d + \nu_1^{\mathrm{alg}}$ and the naive connection $\nabla' = d + \nu_1^{\mathrm{naive}}$, there are no algebraic gauge transformation over any Zariski open subset of $E_{/\mathbb{K}}$ that preserves the group structure on the fiber $\mathbb{L}(\mathsf{S},\mathsf{T})^\wedge$.*

Proof. Suppose there were such a change of gauge g that preserves the group structure, its value would lie in the subgroup $\exp \mathbb{L}(\mathsf{S},\mathsf{T})^\wedge$ of $\operatorname{Aut} \mathbb{L}(\mathsf{S},\mathsf{T})^\wedge$, acting on the fiber $\mathbb{L}(\mathsf{S},\mathsf{T})^\wedge$ by conjugation. In other words, we would have $g : E \dashrightarrow \exp \mathbb{L}(\mathsf{S},\mathsf{T})^\wedge$, with coefficients in $\mathbb{K}(E)$, field of fractions of $\mathcal{O}(E'_{/\mathbb{K}})$, such that

$$\nu_1^{\mathrm{alg}} = -dg \cdot g^{-1} + g\nu_1^{\mathrm{naive}} g^{-1},$$

or equivalently

$$dg = g\nu_1^{\mathrm{naive}} - \nu_1^{\mathrm{alg}} g. \tag{4}$$

This is an equation of 1-forms on E with values in $\operatorname{Der} \mathbb{L}(\mathsf{S},\mathsf{T})^\wedge$. Now let

$$g = 1 + \alpha\mathsf{T} + \beta\mathsf{S} + \gamma\mathsf{T}^2 + \lambda\mathsf{ST} + \mu\mathsf{TS} + \delta\mathsf{S}^2 + \sigma\mathsf{T}^3 + \zeta\mathsf{T}^2\mathsf{S} + \eta\mathsf{TST} + \xi\mathsf{TS}^2 + \tau\mathsf{ST}^2 + \kappa\mathsf{STS} + \epsilon\mathsf{S}^2\mathsf{T} + \iota\mathsf{S}^3 + \cdots$$

[13] The "$-$" sign appears as we regard $-\mathsf{T}$ and S as a basis for $H_1(E)$, dual to $\mathsf{S} = xdx/y$ and $\mathsf{T} = dx/y$ in $H^1(E)$, see Remark 2.2 before Section 2D.

where coefficients $\alpha, \beta, \gamma, \ldots \in \mathbb{K}(E)$ should be regarded as rational functions on the elliptic curve $E_{/\mathbb{K}}$. We substitute g into (4). Now we equate the coefficients up to the third degree of derivations in $\operatorname{Der} \mathbb{L}(\mathsf{S}, \mathsf{T})^\wedge$. We have

$$d\alpha = 0, \quad d\beta = 0, \quad d\gamma = 0, \quad d\delta = 0, \quad d\sigma = 0 \tag{5}$$

$$d\mu = \alpha \frac{dx}{y} + \beta \frac{x\,dx}{y} \tag{6}$$

$$d\lambda = -\beta \frac{x\,dx}{y} - \alpha \frac{dx}{y} \tag{7}$$

$$d\zeta = \gamma \frac{dx}{y} + \mu \frac{x\,dx}{y} + \frac{1}{2}\frac{x\,dx}{y} \tag{8}$$

$$d\eta = -\mu \frac{x\,dx}{y} + \lambda \frac{x\,dx}{y} \tag{9}$$

$$d\xi = \mu \frac{dx}{y} + \delta \frac{x\,dx}{y} \tag{10}$$

$$\cdots \tag{11}$$

From (5), we know that α and β are constants. Taking cohomology classes on both sides of (6), we have

$$\alpha \left[\frac{dx}{y}\right] + \beta \left[\frac{x\,dx}{y}\right] = 0,$$

and easily get $\alpha = \beta = 0$. Thus $d\mu = 0$, and μ is a constant. For the same reason, λ is a constant.

Now taking cohomology classes on both sides of (8) and of (9), we get $\gamma = 0$, and $\lambda = \mu = -\frac{1}{2}$. Similarly, taking cohomology classes on both sides of (10), we get $\mu = \delta = 0$. However, μ cannot be $-\frac{1}{2}$ and 0 at the same time! □

Remark 7.3. If we forget about the group structure on the fiber $\mathbb{L}(\mathsf{S}, \mathsf{T})^\wedge$, we expect that there is an algebraic gauge transformation, defined over $\mathbb{K}$ and meromorphic at the identity when working over $\mathbb{C}$, between the elliptic KZB connection and the naive connection. The reason is that one expects to be able to solve the above (4), if the gauge transformation g is allowed to take value in $\operatorname{Aut} \mathbb{L}(\mathsf{S}, \mathsf{T})^\wedge$. This would indicate that periods of (regularized) iterated integrals constructed from both connections are the same. For some evidence of this, up to degree 5, one can take g to be

$$\begin{aligned} g : \mathsf{S} &\mapsto \mathsf{S} - \tfrac{29}{960} u[\mathsf{T}, [\mathsf{T}, [\mathsf{T}, [\mathsf{T}, \mathsf{S}]]]] - \tfrac{1}{6} x[\mathsf{S}, [\mathsf{T}, [\mathsf{T}, [\mathsf{T}, \mathsf{S}]]]] + \cdots \\ \mathsf{T} &\mapsto \mathsf{T} + \tfrac{1}{2}[\mathsf{T}, [\mathsf{T}, \mathsf{S}]] - \tfrac{1}{6} x[\mathsf{T}, [\mathsf{T}, [\mathsf{T}, [\mathsf{T}, \mathsf{S}]]]] - \tfrac{1}{6}[\mathsf{S}, [\mathsf{T}, [\mathsf{T}, [\mathsf{T}, \mathsf{S}]]]] + \cdots \end{aligned}$$

The form of this seems to suggest that there are (cohomological) obstructions in degrees 3, 5, ... to gauge transform between the elliptic KZB connection and the naive connection while preserving the group structure on $\mathbb{L}(\mathsf{S}, \mathsf{T})^\wedge$.

8. Algebraic connection formula over E''

Recall that we have an analytic local system $(\mathcal{P}, \nabla^{\mathrm{an}})$ of (Lie algebras of) unipotent fundamental groups over E'. The elliptic KZB connection ∇^{an} is obtained by restricting the universal elliptic KZB connection to E'. Note that the analytic formula of the elliptic KZB connection ∇^{an} has regular singularity at the identity with pronilpotent residue. The elliptic KZB connection thus extends naturally from E' to E, and we obtain Deligne's canonical extension $(\overline{\mathcal{P}}, \nabla^{\mathrm{an}})$ of $(\mathcal{P}, \nabla^{\mathrm{an}})$. It is not immediately clear that $(\overline{\mathcal{P}}, \nabla^{\mathrm{an}})$ has an algebraic de Rham structure. The question is to determine whether this canonical extension is defined over $\mathbb{K}$, the field of definition of E. In this section, we show that the elliptic KZB connection ∇^{an} is gauge equivalent to its algebraic counterpart ∇ defined over $\mathbb{K}$, which has regular singularity at the identity with pronilpotent residue. It follows that Deligne's canonical extension $\overline{\mathcal{P}}$ of $\mathcal{P}$ to E is defined over $\mathbb{K}$.

We start with the algebraic connection $\nabla = d + \nu_1^{\mathrm{alg}}$, which is defined to be gauge equivalent to the analytic one ∇^{an} in the last section. Since ν_1^{alg} has irregular singularities at the identity of E, we would like to apply another gauge transformation to make it regular. The reason ν_1^{alg} has irregular singularity is that we introduced a gauge transformation involving E_1, which has a pole at the identity. To cancel this effect and make the connection regular at the identity, we apply a gauge transformation $g_{\mathrm{reg}} = \exp(-(2x^2/y)\mathsf{T})$. Then the connection becomes $\nabla = d + \nu_1^{\mathrm{reg}}$, with 1-form

$$\begin{aligned}
\nu_1^{\mathrm{reg}} &= -dg_{\mathrm{reg}} \cdot g_{\mathrm{reg}}^{-1} + g_{\mathrm{reg}} \nu_1^{\mathrm{alg}}\, g_{\mathrm{reg}}^{-1} \\
&= \left(d\left(\frac{2x^2}{y}\right) - \frac{x\,dx}{y}\right)\mathsf{T} + \exp\left(-\frac{2x^2}{y}\mathsf{T} - \sum_{k=2}^{\infty} \frac{(-\mathsf{T})^k}{k} P_k(x, y)\right) \cdot \mathsf{S} \otimes 2\pi i\, d\xi \\
&= \left(d\left(\frac{2x^2}{y}\right) - \frac{x\,dx}{y}\right)\mathsf{T} + \frac{dx}{y}\mathsf{S} + \sum_{n=1}^{\infty} r_n(x, y) \frac{dx}{y} \mathsf{T}^n \cdot \mathsf{S}.
\end{aligned}$$

Here $\nu_1^{\mathrm{reg}} \in \Omega^1(E'' \log\{\mathrm{id}\}) \otimes \mathbb{L}_{\mathbb{K}}(\mathsf{S}, \mathsf{T})^{\wedge}$ and we get, by direct calculation, rational functions

$$r_n(x, y) = \sum_{a_1 + 2a_2 + 3a_3 + \cdots + na_n = n} \frac{1}{a_1! a_2! a_3! \cdots a_n!} \prod_{k=1}^{n} \left(\frac{(-1)^{k+1} P_k(x, y)}{k}\right)^{a_k} \in \mathcal{O}(E'' \setminus \{\mathrm{id}\}),$$

where $P_1(x, y) := -2x^2/y$ and $\mathcal{O}(E'' \setminus \{\mathrm{id}\}) = \mathcal{O}(E'_y) = \mathcal{O}(E')[y^{-1}]$. Note that the sum for r_n is indexed by the partitions of integer n with no restrictions of the summands. For example, 4 has 5 partitions: 4, $3+1$, $2+2$, $2+1+1$, $1+1+1+1$, so

$$\begin{aligned}
r_4 &= \left(-\frac{P_4}{4}\right) + \frac{1}{1!1!}\left(\frac{P_3}{3}\right) \cdot \left(\frac{P_1}{1}\right) + \frac{1}{2!}\left(-\frac{P_2}{2}\right)^2 + \frac{1}{2!1!}\left(\frac{P_1}{1}\right)^2 \cdot \left(-\frac{P_2}{2}\right) + \frac{1}{4!}\left(\frac{P_1}{1}\right)^4 \\
&= -\frac{1}{4}P_4 + \frac{1}{3}P_3 P_1 + \frac{1}{8}P_2^2 - \frac{1}{4}P_2 P_1^2 + \frac{1}{24}P_1^4
\end{aligned}$$

Remark 8.1. One can use the recurrence relations of the P_k described in Section 3B to find relations among the r_n.

In the next section, we will check that:

Lemma 8.2. *The connection $\nabla = d + \nu_1^{\mathrm{reg}}$ has a regular singularity at the identity with pronilpotent residue.*

Therefore, this connection a priori living on $E'' \setminus \{\mathrm{id}\}$, can be extended naturally across the identity. It is an algebraic connection defined over $\mathbb{K}$ on an algebraic vector bundle $\overline{\mathcal{P}}_{\mathrm{dR}}|_{E''}$ over the open subset E'' of E. This is one part of a vector bundle $\overline{\mathcal{P}}_{\mathrm{dR}}$ over E. The other part $\overline{\mathcal{P}}_{\mathrm{dR}}|_{E'} = \mathcal{P}_{\mathrm{dR}}$ was constructed using the connection $\nabla = d + \nu_1^{\mathrm{alg}}$ in the last section. Now we have trivialized $\overline{\mathcal{P}}_{\mathrm{dR}}$ on an open cover of two different subsets of E. By gluing two trivializations together in terms of the gauge transformation, we have constructed an algebraic vector bundle $\overline{\mathcal{P}}_{\mathrm{dR}}$ over E.

Summarizing results in this part, we get:

Theorem 8.3 (the algebraic de Rham structure $\overline{\mathcal{P}}_{\mathrm{dR}}$ on $\overline{\mathcal{P}}$ over E). *Suppose that $\mathbb{K}$ is a field of characteristic* 0, *embeddable in $\mathbb{C}$. Let E be an elliptic curve defined over $\mathbb{K}$. Then for each embedding $\sigma : \mathbb{K} \hookrightarrow \mathbb{C}$, we have an algebraic vector bundle $\overline{\mathcal{P}}_{\mathrm{dR}}$ over $E_{/\mathbb{K}}$ endowed with connection ∇, and an isomorphism*

$$(\overline{\mathcal{P}}_{\mathrm{dR}}, \nabla) \otimes_{\mathbb{K},\sigma} \mathbb{C} \approx (\overline{\mathcal{P}}, \nabla^{\mathrm{an}}).$$

The algebraic bundle $\overline{\mathcal{P}}_{\mathrm{dR}}$ and its connection ∇ are both defined over $\mathbb{K}$. The $\mathbb{K}$-de Rham structure $(\overline{\mathcal{P}}_{\mathrm{dR}}, \nabla)$ on $(\overline{\mathcal{P}}, \nabla^{\mathrm{an}})$ is explicitly given by the connection formulas for ν_1^{alg} on E' and ν_1^{reg} on E'' above. In particular, the connection ∇ has a regular singularity at the identity.

9. Regular singularity and residue at the identity

In this section, we prove Lemma 8.2 by showing that ν_1^{reg} has regular singularity at the identity, and we compute its residue there.

It is easy to check that analytically $d(2x^2/y) - x\,dx/y$ is holomorphic at the identity. So we are left to check that

$$1 + \sum_{n=1}^{\infty} r_n(x, y)\mathsf{T}^n = \exp\left(-\sum_{k=1}^{\infty} \frac{(-\mathsf{T})^k}{k} P_k(x, y)\right) \tag{12}$$

has a regular singularity at the identity.

Let ξ be the complex coordinate near the identity. Analytically, we need to calculate (in terms of ξ) the principal parts of $P_1 = -2x^2/y$ and P_k's $(k \geq 2)$. The principal part of $P_1 = -2x^2/y$ is $1/(2\pi i\xi)$; the principal part of P_k $(k \geq 2)$ is $1/(2\pi i\xi)^k$, since

$$\begin{aligned} P_k &= (2\pi i)^{-k}(E_k - e_k) \\ &= (2\pi i)^{-k} \sum_{m,n} (\xi + m\tau + n)^{-k} - \sum_{m,n}{}' (m\tau + n)^{-k} \\ &= \frac{1}{(2\pi i)^k \xi^k} + (2\pi i)^{-k} \sum_{m,n}{}' \left(\frac{1}{(\xi + m\tau + n)^k} - \frac{1}{(m\tau + n)^k}\right) \end{aligned}$$

$$= \frac{1}{(2\pi i)^k \xi^k} + (2\pi i)^{-k} \sum_{m,n}' \frac{1}{(m\tau+n)^k} \sum_{l=1}^{\infty} (-1)^l \binom{l+k-1}{k-1} \frac{\xi^l}{(m\tau+n)^l}$$
$$= \frac{1}{(2\pi i\xi)^k} + \sum_{l=1}^{\infty} (-1)^l \binom{l+k-1}{k-1} (2\pi i)^{-(k+l)} e_{k+l}\,(2\pi i\xi)^l.$$

Therefore, (12) is of the following form near $\xi = 0$,

$$\exp\left(-\sum_{k=1}^{\infty} \frac{(-\mathsf{T}/(2\pi i\xi))^k}{k} + \text{holomorphic in } \xi\right) = \exp\left(\ln\left(1+\frac{\mathsf{T}}{2\pi i\xi}\right)\right) \exp\left(\sum_{n=0}^{\infty} a_n(\mathsf{T})(2\pi i\xi)^n\right)$$
$$= \left(1+\frac{\mathsf{T}}{2\pi i\xi}\right) \exp\left(\sum_{n=1}^{\infty} a_n(\mathsf{T})(2\pi i\xi)^n\right),$$

which has a regular singularity at the identity. Here $\forall n \geq 0$, $a_n(\mathsf{T}) \in \mathbb{K}[\mathsf{T}]$ and $a_0(\mathsf{T}) = 0$.

Now it's easy to calculate the residue. Note that $2x^2/y$ is an odd function in ξ, and when expressed in terms of ξ, it has constant term 0 in the holomorphic part; so does each of the P_k's according to their expansions above. Therefore, we know that the holomorphic part in ξ also has constant term 0, and the residue at the identity we are looking for is then

$$\frac{\mathsf{T}}{2\pi i} \exp(0) \cdot \mathsf{S}(2\pi i) = \mathsf{T} \cdot \mathsf{S} = \mathrm{ad}_{[\mathsf{T},\mathsf{S}]},$$

which is in $\mathrm{Der}\,\mathbb{L}(\mathsf{S},\mathsf{T})^\wedge$. Note that $(2\pi i)$ at the end of the first expression above comes from $dx/y = 2\pi i d\xi$.

10. Tannaka theory and a universal unipotent connection over E

Recall that a unipotent object in a tensor category $\mathcal{C}$ with the identity object $\mathbb{1}_{\mathcal{C}}$ is an object V with a filtration in $\mathcal{C}$

$$0 = V_0 \subseteq \cdots \subseteq V_n = V$$

such that each quotient V_j/V_{j-1} is isomorphic to $\mathbb{1}_{\mathcal{C}}^{\oplus k_j}$ for some $k_j \in \mathbb{N}$.

Let E be an elliptic curve defined over $\mathbb{K}$, and fix an embedding $\sigma : \mathbb{K} \hookrightarrow \mathbb{C}$. Let $E' = E - \{\mathrm{id}\}$. Consider the following tensor categories:

(1) *Unipotent Local Systems*

$$\mathcal{C}_F^{\mathrm{B}} := \{\text{unipotent local systems } \mathbb{V}_F \text{ over } E'(\mathbb{C})\},$$

where F is a field of characteristic 0, and the identity object $\mathbb{1}_{\mathcal{C}_F^{\mathrm{B}}}$ is the constant sheaf $F_{E'}$ on $E'(\mathbb{C})$.

(2) *Algebraic de Rham*

$$\mathcal{C}_{\mathbb{K}}^{\mathrm{dR}} := \left\{ \begin{array}{c} \text{unipotent vector bundles } \overline{\mathcal{V}} \text{ over } E_{/\mathbb{K}} \text{ defined over } \mathbb{K} \text{ with a flat connection } \nabla \\ \text{that has regular singularity at the identity with nilpotent residue} \end{array} \right\},$$

where the identity object $\mathbb{1}_{\mathcal{C}^{\mathrm{dR}}_{\mathbb{K}}}$ is the trivial vector bundle $\mathcal{O}_E$ with the trivial connection given by the exterior differential d.

(3) *Analytic de Rham*

$$\mathcal{C}^{\mathrm{an}} := \left\{ \begin{matrix} \text{unipotent vector bundles } \overline{\mathcal{V}}^{\mathrm{an}} \text{ over } E^{\mathrm{an}} \text{ with a flat connection that is holomorphic over } E'(\mathbb{C}), \\ \text{meromorphic over } E(\mathbb{C}) \text{ and has regular singularity at the identity with nilpotent residue} \end{matrix} \right\},$$

where $E^{\mathrm{an}} = E(\mathbb{C})$ is the analytic variety associated to $E_{/\mathbb{K}}$, and the identity object $\mathbb{1}_{\mathcal{C}^{\mathrm{an}}}$ is the trivial vector bundle $\mathcal{O}_{E^{\mathrm{an}}}$ with the trivial connection given by the exterior differential d.

One can define fiber functors for these tensor categories so that they become neutral tannakian categories. Taking the fiber over $x \in E'(\mathbb{C})$ of any object in $\mathcal{C}^{\mathrm{B}}_F$ provides a fiber functor ω_x of $\mathcal{C}^{\mathrm{B}}_F$. By Tannaka duality and the universal property of unipotent completion, the tannakian fundamental group of $\mathcal{C}^{\mathrm{B}}_F$ with respect to the fiber functor ω_x, which we denote by $\pi_1(\mathcal{C}^{\mathrm{B}}_F, \omega_x)$, is the unipotent fundamental group $\pi_1^{\mathrm{un}}(E', x)_F$ over F. We will denote $\pi_1^{\mathrm{un}}(E', x)_{\mathbb{Q}}$ simply by $\pi_1^{\mathrm{un}}(E', x)$.

In the same way, one can define a fiber functor ω_x of $\mathcal{C}^{\mathrm{an}}$ for any $x \in E(\mathbb{C})$, and a fiber functor ω_x of $\mathcal{C}^{\mathrm{dR}}_{\mathbb{K}}$ for any $x \in E(\mathbb{K})$. Note that we can take x to be the identity $\mathrm{id} \in E(\mathbb{K})$. We denote their corresponding tannakian fundamental groups by $\pi_1(\mathcal{C}^{\mathrm{an}}, \omega_x)$ and $\pi_1(\mathcal{C}^{\mathrm{dR}}_{\mathbb{K}}, \omega_x)$ respectively. Our objective is to establish a natural comparison isomorphism between $\pi_1(\mathcal{C}^{\mathrm{an}}, \omega_x)$ and $\pi_1(\mathcal{C}^{\mathrm{dR}}_{\mathbb{K}}, \omega_x) \times_{\mathbb{K}} \mathbb{C}$ for any $x \in E(\mathbb{K})$.

10A. *Extension groups in $\mathcal{C}^{\mathrm{B}}_F$, $\mathcal{C}^{\mathrm{an}}$ and $\mathcal{C}^{\mathrm{dR}}_{\mathbb{K}}$.* We start with a general setting. Let K be a field of characteristic zero. Let $\mathcal{C}$ be a neutral tannakian category over K with a fiber functor ω all of whose objects are unipotent. Denote its identity object by $\mathbb{1}_{\mathcal{C}}$. The tannakian fundamental group of $\mathcal{C}$ with respect to ω, which we denote by $\mathcal{U}$, is a prounipotent group defined over K. Denote its Lie algebra by $\mathfrak{u}$, viewed as a topological Lie algebra. Since the category of $\mathcal{U}$-modules is equivalent to the category of continuous $\mathfrak{u}$-modules, we have

$$H^m_{\mathrm{cts}}(\mathfrak{u}) \cong H^m(\mathcal{U}) \cong \mathrm{Ext}^m_{\mathcal{C}}(\mathbb{1}_{\mathcal{C}}, \mathbb{1}_{\mathcal{C}}).$$

The following is standard.

Proposition 10.1. *Let $\mathfrak{u}$ be a pronilpotent Lie algebra, and denote its abelianization by $H_1(\mathfrak{u})$. Then*

$$H_1(\mathfrak{u}) \cong \mathrm{Hom}(H^1_{\mathrm{cts}}(\mathfrak{u}), K).$$

If $H^2(\mathfrak{u}) = 0$, then $\mathfrak{u}$ is a free Lie algebra.

Therefore, if $\mathrm{Ext}^2_{\mathcal{C}}(\mathbb{1}_{\mathcal{C}}, \mathbb{1}_{\mathcal{C}}) = 0$, then the Lie algebra $\mathfrak{u}$ of the tannakian fundamental group of $\mathcal{C}$ is freely generated by $\mathrm{Ext}^1_{\mathcal{C}}(\mathbb{1}_{\mathcal{C}}, \mathbb{1}_{\mathcal{C}})^*$, the K-dual of $\mathrm{Ext}^1_{\mathcal{C}}(\mathbb{1}_{\mathcal{C}}, \mathbb{1}_{\mathcal{C}})$.

Now we compute extension groups in categories $\mathcal{C}^{\mathrm{B}}_F$, $\mathcal{C}^{\mathrm{an}}$ and $\mathcal{C}^{\mathrm{dR}}_{\mathbb{K}}$.

Lemma 10.2.
$$\mathrm{Ext}^1_{\mathcal{C}}(\mathbb{1}_{\mathcal{C}}, \mathbb{1}_{\mathcal{C}}) \cong \begin{cases} H^1(E(\mathbb{C}); F) & \textit{when } \mathcal{C} = \mathcal{C}^{\mathrm{B}}_F, \\ H^1(E(\mathbb{C}); \mathbb{C}) & \textit{when } \mathcal{C} = \mathcal{C}^{\mathrm{an}}, \\ H^1_{\mathrm{dR}}(E_{/\mathbb{K}}) & \textit{when } \mathcal{C} = \mathcal{C}^{\mathrm{dR}}_{\mathbb{K}}. \end{cases}$$

Proof. The first two cases are well known. The third case can be easily obtained by tensoring $\mathcal{C}_{\mathbb{K}}^{\mathrm{dR}}$ with $\mathbb{C}$ via the fixed embedding $\sigma : \mathbb{K} \hookrightarrow \mathbb{C}$ and invoking Grothendieck's algebraic de Rham theorem, which provides an isomorphism

$$H^1_{\mathrm{dR}}(E_{/\mathbb{K}}) \otimes_{\mathbb{K}} \mathbb{C} \xrightarrow{\sim} H^1(E(\mathbb{C}); \mathbb{C});$$

instead, we provide another proof, explicitly constructing extensions by using our algebraic connection formulas on $\overline{\mathcal{P}}_{\mathrm{dR}}$. Given a global 1-form ω on E, we can define a connection

$$\nabla = d + \begin{pmatrix} 0 & \omega \\ 0 & 0 \end{pmatrix},$$

on the trivial bundle $\mathcal{O}_E \oplus \mathcal{O}_E$. This defines an extension in $\mathrm{Ext}^1_{\mathcal{C}_{\mathbb{K}}^{\mathrm{dR}}}(\mathbb{1}_{\mathcal{C}_{\mathbb{K}}^{\mathrm{dR}}}, \mathbb{1}_{\mathcal{C}_{\mathbb{K}}^{\mathrm{dR}}})$ and gives rise to a map

$$e : H^0(E, \Omega^1_E) \to \mathrm{Ext}^1_{\mathcal{C}_{\mathbb{K}}^{\mathrm{dR}}}(\mathbb{1}_{\mathcal{C}_{\mathbb{K}}^{\mathrm{dR}}}, \mathbb{1}_{\mathcal{C}_{\mathbb{K}}^{\mathrm{dR}}}),$$

which is injective. To see this, we first tensor with $\mathbb{C}$ on both sides of this map. One can then identify the complexified extension group on the right with $H^1(E; \mathbb{C})$ by using monodromy. And the map becomes the inclusion of holomorphic 1-forms on E into $H^1(E; \mathbb{C})$, which is injective.

Suppose we have a vector bundle $(\mathcal{V}, \nabla) \in \mathcal{C}_{\mathbb{K}}^{\mathrm{dR}}$, which is an extension of $(\mathcal{O}_E, d)$ by $(\mathcal{O}_E, d)$. By forgetting the connections on all these bundles, this extension determines a class in $\mathrm{Ext}^1_E(\mathcal{O}_E, \mathcal{O}_E) \cong H^1(E, \mathcal{O}_E)$. This gives rise to a map f and the following sequence

$$0 \to H^0(E, \Omega^1_E) \xrightarrow{e} \mathrm{Ext}^1_{\mathcal{C}_{\mathbb{K}}^{\mathrm{dR}}}(\mathbb{1}_{\mathcal{C}_{\mathbb{K}}^{\mathrm{dR}}}, \mathbb{1}_{\mathcal{C}_{\mathbb{K}}^{\mathrm{dR}}}) \xrightarrow{f} H^1(E, \mathcal{O}_E) \to 0.$$

The result follows if this is a short exact sequence.

Suppose a vector bundle $(\mathcal{V}, \nabla)$ represents a class in $\ker f$, then we have a split extension (without connection)

$$0 \to \mathcal{O}_E \to \mathcal{V} \to \mathcal{O}_E \to 0.$$

Fixing a splitting on $\mathcal{V}$, the connection can be written as

$$\nabla = d + \begin{pmatrix} 0 & \omega \\ 0 & 0 \end{pmatrix},$$

where ω is a global 1-form on E. So we have

$$\ker f = \mathrm{im}\, e.$$

To show f is surjective, we provide here explicitly a vector bundle with connection that corresponds to a nontrivial extension class in $H^1(E, \mathcal{O}_E)$. Recall that the connection ∇ on $\overline{\mathcal{P}}_{\mathrm{dR}}$ is given by algebraic connection formulas

$$\nabla = \begin{cases} d + \nu_1^{\mathrm{alg}} = d - \frac{x\,dx}{y}\mathsf{T} + \frac{dx}{y}\mathsf{S} + \cdots & \text{on } E', \\ d + \nu_1^{\mathrm{reg}} = d + \left(d\left(\frac{2x^2}{y}\right) - \frac{x\,dx}{y}\right)\mathsf{T} + \frac{dx}{y}\mathsf{S} + \cdots & \text{on } E''. \end{cases}$$

The leading terms recorded here provides a connection on the abelianization of $\overline{\mathcal{P}}_{\mathrm{dR}}$. This gives a nontrivial extension of $\mathcal{O}_E$ by $\mathcal{O}_E$, thus corresponds to a nontrivial class in $H^1(E, \mathcal{O}_E)$. □

10B. ***The de Rham tannakian fundamental group $\pi_1(\mathcal{C}^{\mathrm{dR}}_{\mathbb{K}}, \omega_x)$.*** It is well known that there is an equivalence of categories

$$\mathcal{C}^{\mathrm{B}}_{\mathbb{C}} \rightleftarrows \mathcal{C}^{\mathrm{an}}.$$

The right arrow is the functor that takes a unipotent local system $\mathbb{V}$ over E' to Deligne's canonical extension $(\bar{\mathcal{V}}, \nabla)$ of $\mathbb{V} \otimes \mathcal{O}^{\mathrm{an}}_{E'}$, where

$$\nabla : \bar{\mathcal{V}} \to \bar{\mathcal{V}} \otimes \Omega^1_E(\log\{\mathrm{id}\}).$$

The left arrow is the functor obtained by taking locally flat sections of $\mathcal{V}$ over E'. By this equivalence, we obtain an isomorphism between their tannakian fundamental groups

$$\mathrm{comp}_{\mathrm{an,B}} : \pi_1(\mathcal{C}^{\mathrm{an}}, \omega_x) \xrightarrow{\cong} \pi_1(\mathcal{C}^{\mathrm{B}}_{\mathbb{C}}, \omega_x) = \pi_1^{\mathrm{un}}(E', x) \times_{\mathbb{Q}} \mathbb{C} \tag{13}$$

for each $x \in E'(\mathbb{C})$. By Section 4A, as an abstract group, the unipotent fundamental group $\pi_1^{\mathrm{un}}(E', x)_{\mathbb{C}}$ can be identified with its Lie algebra $\mathbb{L}_{\mathbb{C}}(\mathsf{A}, \mathsf{T})^\wedge$, which is the same as $\mathbb{L}_{\mathbb{C}}(\mathsf{S}, \mathsf{T})^\wedge$, where A, S and T are the sections defined in Section 2D.

The local system $\mathcal{P}$ over E' is a pro-object in $\mathcal{C}^{\mathrm{B}}_{\mathbb{C}}$, which is equivalent to an action

$$\pi_1(\mathcal{C}^{\mathrm{B}}_{\mathbb{C}}, \omega_x) \to \mathrm{Aut}\, \mathbb{L}_{\mathbb{C}}(\mathsf{A}, \mathsf{T})^\wedge \tag{14}$$

of the tannakian fundamental group on the fiber of $\mathcal{P}$ over x. This corresponds to the adjoint action of $\mathbb{L}_{\mathbb{C}}(\mathsf{A}, \mathsf{T})^\wedge$ on itself

$$\mathrm{ad} : \mathbb{L}_{\mathbb{C}}(\mathsf{A}, \mathsf{T})^\wedge \to \mathrm{Der}\ \mathbb{L}_{\mathbb{C}}(\mathsf{A}, \mathsf{T})^\wedge. \tag{15}$$

There is another equivalence of categories

$$\mathcal{C}^{\mathrm{dR}}_{\mathbb{C}} \rightleftarrows \mathcal{C}^{\mathrm{an}},$$

where the right arrow is the obvious one, and the left arrow exists by GAGA: since $E^{\mathrm{an}} = E(\mathbb{C})$ is projective, the category of analytic sheaves over E^{an} is equivalent to its algebraic counterpart over $\mathbb{C}$. By this equivalence, we have an isomorphism of tannakian fundamental groups

$$\pi_1(\mathcal{C}^{\mathrm{an}}, \omega_x) \to \pi_1(\mathcal{C}^{\mathrm{dR}}_{\mathbb{C}}, \omega_x)$$

for any $x \in E(\mathbb{C})$. Although it is well known that for each $x \in E(\mathbb{K})$ one can get a canonical $\mathbb{K}$-structure $\pi_1(\mathcal{C}^{\mathrm{dR}}_{\mathbb{K}}, \omega_x)$ on $\pi_1(\mathcal{C}^{\mathrm{dR}}_{\mathbb{C}}, \omega_x)$, we provide an elaborate proof to set up the discussion of universal connection in the next subsection.

Proposition 10.3. *There is a natural comparison isomorphism*

$$\mathrm{comp}_{\mathrm{an,dR}} : \pi_1(\mathcal{C}^{\mathrm{an}}, \omega_x) \to \pi_1(\mathcal{C}^{\mathrm{dR}}_{\mathbb{K}}, \omega_x) \times_{\mathbb{K}} \mathbb{C}$$

for any $x \in E(\mathbb{K})$.

Proof. This map $\mathrm{comp}_{\mathrm{an,dR}}$ is induced from the functor of tensoring with $\mathbb{C}$ by using the fixed embedding $\sigma : \mathbb{K} \hookrightarrow \mathbb{C}$:

$$\mathcal{C}^{\mathrm{dR}}_{\mathbb{K}} \otimes \mathbb{C} \to \mathcal{C}^{\mathrm{dR}}_{\mathbb{C}} \simeq \mathcal{C}^{\mathrm{an}}.$$

We study it by working with a special object. In Section 8, we constructed such an object: an algebraic vector bundle $(\overline{\mathcal{P}}_{\mathrm{dR}}, \nabla)$ over E with a connection ∇ defined over $\mathbb{K}$. It is a pro-object in $\mathcal{C}^{\mathrm{dR}}_{\mathbb{K}}$, and corresponds to an action

$$\pi_1(\mathcal{C}^{\mathrm{dR}}_{\mathbb{K}}, \omega_x) \to \operatorname{Aut} \mathbb{L}_{\mathbb{K}}(\mathsf{S}, \mathsf{T})^\wedge \tag{16}$$

of the tannakian fundamental group on the fiber over x. Recall from Theorem 8.3 that

$$(\overline{\mathcal{P}}_{\mathrm{dR}}, \nabla) \otimes_{\mathbb{K}} \mathbb{C} \approx (\overline{\mathcal{P}}, \nabla^{\mathrm{an}}),$$

where $\overline{\mathcal{P}}$ is Deligne's canonical extension of $\mathcal{P}$ over E' to E. Therefore, after tensoring with $\mathbb{C}$, we obtain the object $\mathcal{P}$ in $\mathcal{C}^{\mathrm{an}}$, which, by (13) and (14), is equivalent to an action

$$\pi_1(\mathcal{C}^{\mathrm{an}}, \omega_x) \to \operatorname{Aut} \mathbb{L}_{\mathbb{C}}(\mathsf{S}, \mathsf{T})^\wedge.$$

This action factors through the action given by (16) $\times_{\mathbb{K}} \mathbb{C}$, that is, we have a diagram

$$\begin{array}{ccc} \pi_1(\mathcal{C}^{\mathrm{an}}, \omega_x) & \xrightarrow{\mathrm{comp}_{\mathrm{an,dR}}} & \pi_1(\mathcal{C}^{\mathrm{dR}}_{\mathbb{K}}, \omega_x) \times_{\mathbb{K}} \mathbb{C} \\ & \searrow & \downarrow \\ & & \operatorname{Aut} \mathbb{L}_{\mathbb{C}}(\mathsf{S}, \mathsf{T})^\wedge \end{array}$$

Note that the functor that takes a unipotent group to its Lie algebra is an equivalence of categories between the category of unipotent $\mathbb{K}$-groups and the category of nilpotent Lie algebras over $\mathbb{K}$. The above diagram is thus equivalent to the following diagram

$$\begin{array}{ccc} \mathbb{L}_{\mathbb{C}}(\mathsf{A}, \mathsf{T})^\wedge & \longrightarrow & \mathfrak{u}(\mathcal{C}^{\mathrm{dR}}_{\mathbb{K}}, \omega_x) \otimes_{\mathbb{K}} \mathbb{C} \\ & \overset{\mathrm{ad}}{\hookrightarrow} & \downarrow \\ & & \operatorname{Der} \mathbb{L}_{\mathbb{C}}(\mathsf{A}, \mathsf{T})^\wedge \end{array}$$

where $\mathfrak{u}(\mathcal{C}^{\mathrm{dR}}_{\mathbb{K}}, \omega_x)$ denotes the Lie algebra of $\pi_1(\mathcal{C}^{\mathrm{dR}}_{\mathbb{K}}, \omega_x)$. Since the adjoint action $\mathrm{ad} : \mathbb{L}_{\mathbb{C}}(\mathsf{A}, \mathsf{T})^\wedge \to \operatorname{Der} \mathbb{L}_{\mathbb{C}}(\mathsf{A}, \mathsf{T})^\wedge$ from (15) is injective, the top row of the previous diagram

$$\mathrm{comp}_{\mathrm{an,dR}} : \pi_1(\mathcal{C}^{\mathrm{an}}, \omega_x) \to \pi_1(\mathcal{C}^{\mathrm{dR}}_{\mathbb{K}}, \omega_x) \times_{\mathbb{K}} \mathbb{C}$$

must also be injective. The surjectivity of this map follows from the fact that the Lie algebra $\mathfrak{u}(\mathcal{C}^{\mathrm{dR}}_{\mathbb{K}}, \omega_x)$ is generated by the $\mathbb{K}$-dual $H^1_{\mathrm{dR}}(E_{/\mathbb{K}})^*$ of $H^1_{\mathrm{dR}}(E_{/\mathbb{K}})$, see discussion in Section 10A. □

Remark 10.4. One can choose x to be a tangential base point. For example, one can take the fiber functor to be the fiber at the unit tangent vector $\vec{\mathrm{v}}$ at the identity of E. We will denote this fiber functor by $\omega_{\vec{\mathrm{v}}}$. For an admissible variation of Hodge structures, this amounts to taking the limit mixed Hodge structure associated to the tangent vector, see the natural definition given in [Hain 1987]. See also [Deligne 1989, Sections 15.3–15.12] for tangential base points and [Hain 2013, Section 16] for their relations to limit mixed Hodge structures.

Corollary 10.5. *There is an isomorphism of groups over* $\mathbb{K}$

$$\pi_1(\mathcal{C}^{\mathrm{dR}}_{\mathbb{K}}, \omega_x) \cong \exp \mathbb{L}_{\mathbb{K}}(\mathsf{S}, \mathsf{T})^\wedge$$

for any $x \in E(\mathbb{K})$.

Remark 10.6. One can establish the isomorphism in a different way. By Deligne [1989, Corollary 10.43], in the unipotent case, the tannakian fundamental groupoid is compatible with extension of scalars. In particular, for our category $\mathcal{C}^{\mathrm{dR}}_{\mathbb{K}}$, given any $x \in E(\mathbb{K})$, restricting its tannakian fundamental groupoid to a diagonal point (x, x) gives a tannakian fundamental group defined over $\mathbb{K}$, which is also compatible with extension of scalars, i.e., $\pi_1(\mathcal{C}^{\mathrm{dR}}_{\mathbb{K}}) \times_{\mathbb{K}} \mathbb{C} \cong \pi_1(\mathcal{C}^{\mathrm{dR}}_{\mathbb{C}})$. Therefore, one obtains an isomorphism

$$\pi_1(\mathcal{C}^{\mathrm{an}}, \omega_x) \to \pi_1(\mathcal{C}^{\mathrm{dR}}_{\mathbb{K}}, \omega_x) \times_{\mathbb{K}} \mathbb{C}.$$

10C. ***Universal unipotent connection over an elliptic curve*** $\boldsymbol{E_{/\mathbb{K}}}$**.** Using the explicit universal connection ∇ on $\overline{\mathcal{P}}_{\mathrm{dR}}$, we provide an explicit construction of the $\mathbb{K}$-connection that has regular singularity at the identity of $E_{/\mathbb{K}}$ on a unipotent vector bundle $\overline{\mathcal{V}}$ [14] in $\mathcal{C}^{\mathrm{dR}}_{\mathbb{K}}$ which, by Corollary 10.5, corresponds to a unipotent representation

$$\rho : \exp \mathbb{L}_{\mathbb{K}}(\mathsf{S}, \mathsf{T})^\wedge \to \mathrm{Aut}(V).$$

This is achieved by composing the universal connection forms with the representation ρ.

Given a unipotent vector bundle $\overline{\mathcal{V}}$ over $E_{/\mathbb{K}}$ in $\mathcal{C}^{\mathrm{dR}}_{\mathbb{K}}$. Choose the fiber functor $\omega_{\vec{\mathrm{v}}}$ over the unit tangent vector $\vec{\mathrm{v}}$ at the identity of E and denote by $V := V_{\vec{\mathrm{v}}}$ the fiber over the tangent vector $\vec{\mathrm{v}}$ at the identity (see Remark 10.4). This vector bundle $\overline{\mathcal{V}}$ corresponds to a unipotent representation

$$\rho : \exp \mathbb{L}_{\mathbb{K}}(\mathsf{S}, \mathsf{T})^\wedge \to \mathrm{Aut}(V),$$

and equivalently a Lie algebra homomorphism

$$\log \rho : \mathbb{L}_{\mathbb{K}}(\mathsf{S}, \mathsf{T})^\wedge \to \mathrm{End}(V).$$

Recall that we have defined 1-forms

$$\nu_1^{\mathrm{alg}} \in \Omega^1(E') \otimes \mathbb{L}_{\mathbb{K}}(\mathsf{S}, \mathsf{T})^\wedge \quad \text{and} \quad \nu_1^{\mathrm{reg}} \in \Omega^1(E'' \log\{\mathrm{id}\}) \otimes \mathbb{L}_{\mathbb{K}}(\mathsf{S}, \mathsf{T})^\wedge$$

in Section 7 and Section 8, respectively. They are gauge equivalent on $E' \cap E''$ via the transformation

$$g_{\mathrm{reg}} : E' \cap E'' \to \exp \mathbb{L}_{\mathbb{K}}(\mathsf{S}, \mathsf{T})^\wedge \subset \mathrm{Aut}\, \mathbb{L}_{\mathbb{K}}(\mathsf{S}, \mathsf{T})^\wedge.$$

Define 1-forms

$$\Omega'_V := (1 \otimes \log \rho) \circ \nu_1^{\mathrm{alg}} \in \Omega^1(E') \otimes \mathrm{End}(V)$$

[14] One should think of this bundle as Deligne's canonical extension to E of $\mathcal{V}$ over E'.

and

$$\Omega''_V := (1 \otimes \log \rho) \circ \nu_1^{\text{reg}} \in \Omega^1(E'' \log\{\text{id}\}) \otimes \text{End}(V).$$

Over E' and E'', we endow trivial bundles

$$\begin{array}{ccc} V \times E' & \text{and} & V \times E'' \\ \downarrow & & \downarrow \\ E' & & E'' \end{array}$$

with connections $\nabla = d + \Omega'_V$ and $\nabla = d + \Omega''_V$, respectively. Define

$$g_V : E' \cap E'' \to \text{Aut}(V)$$

by $g_V := \exp(\log \rho \circ \log g_{\text{reg}})$, then Ω'_V and Ω''_V are gauge equivalent on $E' \cap E''$ via g_V. After gluing these two trivial bundles by the gauge transformation g_V, we obtain a connection ∇ on $\bar{\mathcal{V}}$ defined over $\mathbb{K}$ such that

$$\nabla : \bar{\mathcal{V}} \to \bar{\mathcal{V}} \otimes \Omega^1_E(\log\{\text{id}\}).$$

Part III. Universal elliptic KZB connection — algebraic formula

Levin and Racinet [2007, Section 5] sketched a proof to show that the bundle $\mathcal{P}$ over $\mathcal{E}$ and its connection, the universal elliptic KZB connection, are defined over $\mathbb{Q}$. However, just as in the case of a single elliptic curve, their work is incomplete in that their connection formula has irregular singularities along the identity section of $\mathcal{E}$.

We show that after an algebraic change of gauge, the universal elliptic KZB connection has regular singularities along the identity section of $\mathcal{E}$ and the nodal cubic. Since all these data are defined over $\mathbb{Q}$, we have completed the work.

Similar to the previous part, we compute explicitly the connection formula in terms of algebraic coordinates on $\mathcal{E}$. We resolve the issue of irregular singularities by trivializing the bundle on two open subsets $\mathcal{E}'$ and $\mathcal{E}''$ of $\mathcal{E}$, where $\mathcal{E}'$ is obtained from $\mathcal{E}$ by removing the identity section,[15] and $\mathcal{E}''$ is obtained from $\mathcal{E}$ by removing three sections that correspond to three nontrivial order 2 elements on each fiber. On both open subsets, the algebraic connection formulas are defined over $\mathbb{Q}$, and the one on $\mathcal{E}''$ has regular singularities along the identity section. Note that the singularities around the nodal cubic are regular on both open subsets, and the gauge transformation on their intersection is compatible with the canonical extension $\overline{\mathcal{P}}$ of $\mathcal{P}$ over $\mathcal{E}$ to $\bar{\mathcal{E}}$. One can think of the universal elliptic KZB connection as an algebraic connection on an algebraic vector bundle $\overline{\mathcal{P}}_{\text{dR}}$ over $\bar{\mathcal{E}}$, which is defined over $\mathbb{Q}$ with regular singularities along boundary divisors. Therefore, we have constructed a $\mathbb{Q}$-de Rham structure $\overline{\mathcal{P}}_{\text{dR}}$ on $\overline{\mathcal{P}}$ over $\bar{\mathcal{E}}$.

[15] It is $\mathcal{M}_{1,2}$ as defined in Section 1B.

11. Algebraic connection formula over $\mathcal{E}'$

In Section 5, we defined the universal elliptic KZB connection ∇^{an} on the bundle $\mathcal{P}$ over $\mathcal{E}'$ analytically. This bundle $\mathcal{P}$ can be pulled back to a bundle over $\mathcal{M}^{\mathrm{an}}_{1,1+\vec{1}}$ with connection, which we also denote by ∇^{an}. In this section, we will write this connection in terms of algebraic coordinates x, y, u, v on $\mathcal{M}_{1,1+\vec{1}}$ (defined in Section 1A). The connection is $\mathbb{G}_m$-invariant, and is trivial on each fiber of $\mathcal{M}_{1,1+\vec{1}} \to \mathcal{M}_{1,2}$, thus descends to a connection on $\mathcal{M}_{1,2} = \mathcal{E}'$.

As in the case of a single elliptic curve, fiber by fiber, we apply the gauge transformation of

$$g_{\mathrm{alg}}(\xi,\tau) = \exp\left(-\frac{E_1}{2\pi i}\mathsf{T}\right)$$

with both g_{alg} and E_1 having the extra variable τ. After the gauge transformation, the connection

$$\nabla^{\mathrm{an}} = d + \omega$$

transforms into

$$\nabla = d + \omega_{\mathrm{alg}} = d - dg_{\mathrm{alg}} \cdot g_{\mathrm{alg}}^{-1} + g_{\mathrm{alg}}\omega g_{\mathrm{alg}}^{-1}.$$

So using Formulas 3.3, 3.6 and 3.7 and Lemma 9.3 in [Hain 2013] we have

$$\begin{aligned}
\omega_{\mathrm{alg}} &= -dg_{\mathrm{alg}} \cdot g_{\mathrm{alg}}^{-1} + g_{\mathrm{alg}} \cdot \left(2\pi i\, d\tau \otimes \mathsf{A}\frac{\partial}{\partial \mathsf{T}}\right) + g_{\mathrm{alg}}\psi g_{\mathrm{alg}}^{-1} + g_{\mathrm{alg}}\nu g_{\mathrm{alg}}^{-1} \\
&= \frac{1}{2\pi i}\left(\frac{\partial E_1}{\partial \xi}d\xi + \frac{\partial E_1}{\partial \tau}d\tau\right)\mathsf{T} + 2\pi i\, d\tau \otimes \mathsf{A}\frac{\partial}{\partial \mathsf{T}} + \psi \\
&\quad + \frac{1-\exp(-E_1/(2\pi i)\mathsf{T})}{\mathsf{T}} \cdot \mathsf{A} \otimes 2\pi i d\tau + \exp\left(-\frac{E_1\mathsf{T}}{2\pi i}\right)\mathsf{T}F^{\mathrm{Zag}}(2\pi i\xi, \mathsf{T}, \tau) \cdot \mathsf{A} \otimes d\xi \\
&\quad + \exp\left(-\frac{E_1\mathsf{T}}{2\pi i}\right)\left(\frac{1}{\mathsf{T}} + \mathsf{T}\frac{\partial F^{\mathrm{Zag}}}{\partial \mathsf{T}}(2\pi i\xi, \mathsf{T}, \tau)\right) \cdot \mathsf{A} \otimes 2\pi i d\tau \\
&= \frac{1}{2\pi i}\left(-E_2 d\xi + \frac{1}{2\pi i}(E_3 - E_1E_2)d\tau\right)\mathsf{T} + 2\pi i\, d\tau \otimes \mathsf{A}\frac{\partial}{\partial \mathsf{T}} + \psi \\
&\quad + \frac{1-\exp(-E_1/(2\pi i)\mathsf{T})}{\mathsf{T}} \cdot \mathsf{A} \otimes 2\pi i d\tau + \exp\left(-\sum_{k=2}^{\infty}\frac{(-\mathsf{T})^k}{k}P_k(\xi,\tau)\right) \cdot \mathsf{A} \otimes 2\pi i d\xi \\
&\quad + 2\pi i d\tau \otimes \left[\frac{\exp(-E_1/(2\pi i)\mathsf{T})}{\mathsf{T}} + \exp\left(-\sum_{k=2}^{\infty}\frac{(-\mathsf{T})^k}{k}P_k(\xi,\tau)\right)\left(\sum_{k=1}^{\infty}(-\mathsf{T})^{k-1}P_k(\xi,\tau) - \frac{1}{\mathsf{T}}\right)\right] \cdot \mathsf{A} \\
&= \left(-(2\pi i)^{-2}(E_2 - e_2)\mathsf{T} + \exp\left(-\sum_{k=2}^{\infty}\frac{(-\mathsf{T})^k}{k}P_k(\xi,\tau)\right) \cdot \mathsf{S}\right) \otimes 2\pi i\left(d\xi + \frac{1}{2\pi i}E_1 d\tau\right) \\
&\quad + (2\pi i)^{-3}E_3\mathsf{T} \otimes 2\pi i d\tau + 2\pi i\, d\tau \otimes \mathsf{A}\frac{\partial}{\partial \mathsf{T}} + \psi \\
&\quad + \left[\exp\left(-\sum_{k=2}^{\infty}\frac{(-\mathsf{T})^k}{k}P_k(\xi,\tau)\right)\left(\sum_{k=2}^{\infty}(-\mathsf{T})^{k-1}P_k(\xi,\tau) - \frac{1}{\mathsf{T}}\right) + \frac{1}{\mathsf{T}}\right] \cdot \mathsf{S} \otimes 2\pi i d\tau
\end{aligned}$$

Recall the map from Section 1B

$$(\mathbb{C}\times\mathfrak{h})-\Lambda_{\mathfrak{h}}\to\mathcal{M}^{\mathrm{an}}_{1,1+\vec{1}}=\{(x,y,u,v)\in\mathbb{C}^2\times\mathbb{C}^2: y^2=4x^3-ux-v,\,(u,v)\neq(0,0)\}$$
$$(\xi,\tau)\mapsto\bigl(P_2(\xi,\tau),-2P_3(\xi,\tau),20G_4(\tau),\tfrac{7}{3}G_6(\tau)\bigr)$$

that induces an isomorphism $\mathrm{SL}_2(\mathbb{Z})\ltimes\mathbb{Z}^2\backslash\backslash((\mathbb{C}\times\mathfrak{h})-\Lambda_{\mathfrak{h}})\cong\mathbb{G}_m\backslash\backslash\mathcal{M}^{\mathrm{an}}_{1,1+\vec{1}}$. By pulling back through this map, we identify some algebraic forms with their analytic counterparts appeared in the formula above in the following

Lemma 11.1. *Set $\alpha=2udv-3vdu$, $\Delta=u^3-27v^2$. Then*

$$2\pi i\,d\tau=\frac{3\alpha}{2\Delta}\quad\textit{and}\quad 2\pi i\left(d\xi+\frac{1}{2\pi i}E_1d\tau\right)=\frac{dx}{y}-\frac{6x^2-u}{y}\frac{\alpha}{2\Delta}-\frac{1}{6}\frac{d\Delta}{\Delta}\frac{x}{y}.$$

Proof. Direct computation from [Levin and Racinet 2007, Proposition 5.2.3]. □

Recall from Remark 3.4 that $P_k(\xi,\tau)=(2\pi i)^{-k}(E_k-e_k)$, $k\geq 2$ can be written as rational polynomials of $x=P_2(\xi,\tau)$, $y=-2P_3(\xi,\tau)$, $u=20G_4(\tau)$ and $v=\frac{7}{3}G_6(\tau)$, i.e., for all $k\geq 2$, it can be written as $P_k(x,y,u,v)\in\mathbb{Q}[x,y,u,v]$. Combining this with Lemma 11.1, we only need to show that in terms of basis elements T and S,

$$d+2\pi i\,d\tau\otimes\mathsf{A}\frac{\partial}{\partial\mathsf{T}}+\psi$$

is algebraic. But with respect to the above framing, $d+2\pi i\,d\tau\otimes\mathsf{A}\partial/\partial\mathsf{T}$ transforms to [Hain 2013, Proposition 19.6]

$$d+\left(-\frac{1}{12}\frac{d\Delta}{\Delta}\mathsf{T}+\frac{3\alpha}{2\Delta}\mathsf{S}\right)\frac{\partial}{\partial\mathsf{T}}+\left(-\frac{u\alpha}{8\Delta}\mathsf{T}+\frac{1}{12}\frac{d\Delta}{\Delta}\mathsf{S}\right)\frac{\partial}{\partial\mathsf{S}},\tag{17}$$

and ψ transforms to

$$\sum_{m\geq 1}\left(\frac{1}{(2m)!}\frac{3\alpha}{2\Delta}p_{2m+2}(u,v)\otimes\sum_{\substack{j+k=2m+1\\ j,k>0}}(-1)^j[\mathrm{ad}^j_{\mathsf{T}}(\mathsf{S}),\mathrm{ad}^k_{\mathsf{T}}(\mathsf{S})]\frac{\partial}{\partial\mathsf{S}}\right),\tag{18}$$

where G_{2m+2} is replaced by $p_{2m+2}(u,v)\in\mathbb{Q}[u,v]$ ($p_{2m}(u,v)$'s are polynomials defined by $G_{2m}(\tau)=p_{2m}(20G_4(\tau),7G_6(\tau)/3)$, where G_{2m} is a normalized Eisenstein series of weight $2m$), and $\mathrm{ad}^j_{\mathsf{T}}$ denotes the operation that takes the adjoint action of T repeatedly for j times. Note that every derivation $\delta\in\mathrm{Der}\,\mathbb{L}_{\mathbb{Q}}(\mathsf{S},\mathsf{T})^\wedge$ can be written uniquely in the form

$$\delta=\delta(\mathsf{S})\frac{\partial}{\partial\mathsf{S}}+\delta(\mathsf{T})\frac{\partial}{\partial\mathsf{T}},$$

as it is determined by its values on S and T.

So the algebraic 1-form of the universal elliptic KZB connection is given by

$$\begin{aligned}\omega_{\mathrm{alg}} = &\left(-\frac{1}{12}\frac{d\Delta}{\Delta}\mathsf{T}+\frac{3\alpha}{2\Delta}\mathsf{S}\right)\frac{\partial}{\partial\mathsf{T}}+\left(-\frac{u\alpha}{8\Delta}\mathsf{T}+\frac{1}{12}\frac{d\Delta}{\Delta}\mathsf{S}\right)\frac{\partial}{\partial\mathsf{S}}+\left(-\frac{x\,dx}{y}+\frac{1}{4}\frac{\alpha}{\Delta}\frac{ux+3v}{y}+\frac{1}{6}\frac{d\Delta}{\Delta}\frac{x^2}{y}\right)\mathsf{T}\\ &+\exp\left(-\sum_{k=2}^{\infty}\frac{(-\mathsf{T})^k}{k}P_k(x,y,u,v)\right)\cdot\mathsf{S}\left(\frac{dx}{y}-\frac{6x^2-u}{y}\frac{\alpha}{2\Delta}-\frac{1}{6}\frac{d\Delta}{\Delta}\frac{x}{y}\right)\\ &+\left[\exp\left(-\sum_{k=2}^{\infty}\frac{(-\mathsf{T})^k}{k}P_k(x,y,u,v)\right)\left(\sum_{k=2}^{\infty}(-\mathsf{T})^{k-1}P_k(x,y,u,v)-\frac{1}{\mathsf{T}}\right)+\frac{1}{\mathsf{T}}\right]\cdot\mathsf{S}\frac{3\alpha}{2\Delta}\\ &+\sum_{m\ge1}\left(\frac{1}{(2m)!}\frac{3\alpha}{2\Delta}p_{2m+2}(u,v)\otimes\sum_{j+k=2m+1}\sum_{j,k>0}(-1)^j[\mathrm{ad}^j_{\mathsf{T}}(\mathsf{S}),\mathrm{ad}^k_{\mathsf{T}}(\mathsf{S})]\frac{\partial}{\partial\mathsf{S}}\right)\\ =&\left(-\frac{1}{12}\frac{d\Delta}{\Delta}\mathsf{T}+\frac{3\alpha}{2\Delta}\mathsf{S}\right)\frac{\partial}{\partial\mathsf{T}}+\left(-\frac{u\alpha}{8\Delta}\mathsf{T}+\frac{1}{12}\frac{d\Delta}{\Delta}\mathsf{S}\right)\frac{\partial}{\partial\mathsf{S}}\\ &+\left(-\frac{x\,dx}{y}+\frac{1}{4}\frac{\alpha}{\Delta}\frac{ux+3v}{y}+\frac{1}{6}\frac{d\Delta}{\Delta}\frac{x^2}{y}\right)\mathsf{T}+\left(\frac{dx}{y}-\frac{6x^2-u}{y}\frac{\alpha}{2\Delta}-\frac{1}{6}\frac{d\Delta}{\Delta}\frac{x}{y}\right)\mathsf{S}\\ &+\sum_{n\ge2}\left(\frac{dx}{y}-\frac{6x^2-u}{y}\frac{\alpha}{2\Delta}-\frac{1}{6}\frac{d\Delta}{\Delta}\frac{x}{y}+(n-1)\frac{3\alpha}{2\Delta}\right)q_n(x,y,u,v)\ \mathsf{T}^n\cdot\mathsf{S}\\ &+\sum_{m\ge1}\left(\frac{1}{(2m)!}\frac{3\alpha}{2\Delta}p_{2m+2}(u,v)\otimes\sum_{j+k=2m+1}\sum_{j,k>0}(-1)^j[\mathsf{T}^j\cdot\mathsf{S},\mathsf{T}^k\cdot\mathsf{S}]\frac{\partial}{\partial\mathsf{S}}\right)\end{aligned}$$

where $\Delta=u^3-27v^2$, $\alpha=2u\,dv-3v\,du$, $q_n(x,y,u,v)\in\mathbb{Q}[x,y,u,v]$ $(n\ge2)$ are essentially the same polynomials as in Section 7 but with two more variables u,v (previously u,v are fixed as the elliptic curve is fixed) and $p_{2m}(u,v)\in\mathbb{Q}[u,v]$ are polynomials we just defined. This 1-form takes value in $\mathrm{Der}\,\mathbb{L}_{\mathbb{Q}}(\mathsf{S},\mathsf{T})^\wedge$. We view $\mathbb{L}_{\mathbb{Q}}(\mathsf{S},\mathsf{T})^\wedge$ as a Lie subalgebra of $\mathrm{Der}\,\mathbb{L}_{\mathbb{Q}}(\mathsf{S},\mathsf{T})^\wedge$ via the adjoint action, and T^n acts on $\mathbb{L}_{\mathbb{Q}}(\mathsf{S},\mathsf{T})^\wedge$ as $\mathrm{ad}^n_{\mathsf{T}}$.

12. Algebraic connection formula over $\mathcal{E}''$

As in the single elliptic curve case, we apply the gauge transformation $g_{\mathrm{reg}}=\exp(-(2x^2/y)\mathsf{T})$ to the previous formula for the algebraic 1-form, and obtain the algebraic 1-form

$$\begin{aligned}\omega_{\mathrm{reg}} &= -dg_{\mathrm{reg}}\cdot g_{\mathrm{reg}}^{-1}+g_{\mathrm{reg}}\omega_{\mathrm{alg}}g_{\mathrm{reg}}^{-1}\\ &=\left(-\frac{1}{12}\frac{d\Delta}{\Delta}\mathsf{T}+\frac{3\alpha}{2\Delta}\mathsf{S}\right)\frac{\partial}{\partial\mathsf{T}}+\left(-\frac{u\alpha}{8\Delta}\mathsf{T}+\frac{1}{12}\frac{d\Delta}{\Delta}\mathsf{S}\right)\frac{\partial}{\partial\mathsf{S}}\\ &\quad+\left[\left(d\left(\frac{2x^2}{y}\right)-\frac{x\,dx}{y}\right)+\frac{1}{4}\frac{\alpha}{\Delta}\frac{ux+3v}{y}\right]\mathsf{T}+\left(\frac{dx}{y}+\frac{1}{y}\frac{u\alpha}{2\Delta}-\frac{1}{6}\frac{d\Delta}{\Delta}\frac{x}{y}\right)\mathsf{S}\\ &\quad+\sum_{n\ge1}\left(\frac{dx}{y}+\frac{1}{y}\frac{u\alpha}{2\Delta}-\frac{1}{6}\frac{d\Delta}{\Delta}\frac{x}{y}+(n-1)\frac{3\alpha}{2\Delta}\right)r_n(x,y,u,v)\mathsf{T}^n\cdot\mathsf{S}\\ &\quad+\sum_{m\ge1}\left(\frac{1}{(2m)!}\frac{3\alpha}{2\Delta}p_{2m+2}(u,v)\otimes\sum_{j+k=2m+1}\sum_{j,k>0}(-1)^j[\mathsf{T}^j\cdot\mathsf{S},\mathsf{T}^k\cdot\mathsf{S}]\frac{\partial}{\partial\mathsf{S}}\right)\end{aligned}$$

where $r_n(x, y, u, v) \in \mathbb{Q}(x, y, u, v)$ $(n \geq 2)$ are essentially the same rational functions as in Section 8 but with two more variables u, v.

Note that the $\mathbb{G}_m$-action of λ multiplies T by λ, and S by λ^{-1}. It is easy to check that both connection forms ω_{alg} and ω_{reg} are $\mathbb{G}_m$-invariant. One can also show that the latter connection form ω_{reg} has regular singularity along the identity section, and along the nodal cubic; the residue of the connection around the identity section is $\operatorname{ad}_{[\mathsf{T},\mathsf{S}]}$, which is pronilpotent.

Just like the single elliptic curve case, we can use both connections ω_{alg} and ω_{reg} with the gauge transformation g_{reg} between them to construct a vector bundle $\mathcal{P}_{\text{dR}}$ over $\mathcal{E}_{/\mathbb{Q}}$. Since both connection forms are defined over $\mathbb{Q}$ and have regular singularities along the nodal cubic, we can extend $\mathcal{P}_{\text{dR}}$ to $\bar{\mathcal{E}}_{/\mathbb{Q}}$ and obtain an algebraic vector bundle $\overline{\mathcal{P}}_{\text{dR}}$.

Let $(\overline{\mathcal{P}}, \nabla^{\text{an}})$ be Deligne's canonical extension to $\bar{\mathcal{E}}$ of the bundle $\mathcal{P}$ of (Lie algebras of) unipotent fundamental groups over $\mathcal{E}'$. We have

Theorem 12.1 (the $\mathbb{Q}$-de Rham structure $\overline{\mathcal{P}}_{\text{dR}}$ on $\overline{\mathcal{P}}$ over $\bar{\mathcal{E}}$). *There is an algebraic vector bundle $\overline{\mathcal{P}}_{\text{dR}}$ over $\bar{\mathcal{E}}_{/\mathbb{Q}}$ endowed with connection ∇, and an isomorphism*

$$(\overline{\mathcal{P}}_{\text{dR}}, \nabla) \otimes_{\mathbb{Q}} \mathbb{C} \approx (\overline{\mathcal{P}}, \nabla^{\text{an}}).$$

The algebraic bundle $\overline{\mathcal{P}}_{\text{dR}}$ and its connection ∇ are both defined over $\mathbb{Q}$. The $\mathbb{Q}$-de Rham structure $(\overline{\mathcal{P}}_{\text{dR}}, \nabla)$ on $(\overline{\mathcal{P}}, \nabla^{\text{an}})$ is explicitly given by the connection formulas for ω_{alg} on $\mathcal{E}'$ and ω_{reg} on $\mathcal{E}''$ above. In particular, the connection ∇ has regular singularities along boundary divisors, the identity section and the nodal cubic.

Acknowledgments

I would like to thank my advisor, Richard Hain, for introducing me this problem and providing numerous suggestions and discussions in writing this paper. I would like to thank Francis Brown for discussions, especially on Section 7. I would also like to thank Jin Cao, Benjamin Enriquez, Minhyong Kim, Nils Matthes and Alex Saad for their interest in the paper. Finally, I would like to thank the referees for their thorough reading and useful comments on the manuscript.

References

[Beilinson and Deligne 1994] A. Beĭlinson and P. Deligne, "Interprétation motivique de la conjecture de Zagier reliant polylogarithmes et régulateurs", pp. 97–121 in *Motives, II* (Seattle, 1991), edited by U. Jannsen et al., Proc. Sympos. Pure Math. **55**, Amer. Math. Soc., Providence, RI, 1994. MR Zbl

[Beilinson and Levin 1994] A. Beĭlinson and A. Levin, "The elliptic polylogarithm", pp. 123–190 in *Motives, II* (Seattle, 1991), edited by U. Jannsen et al., Proc. Sympos. Pure Math. **55**, Amer. Math. Soc., Providence, RI, 1994. MR Zbl

[Brown and Levin 2011] F. C. S. Brown and A. Levin, "Multiple elliptic polylogarithms", preprint, 2011. arXiv

[Calaque et al. 2009] D. Calaque, B. Enriquez, and P. Etingof, "Universal KZB equations: the elliptic case", pp. 165–266 in *Algebra, arithmetic, and geometry: in honor of Yu. I. Manin, I*, edited by Y. Tschinkel and Y. Zarhin, Progr. Math. **269**, Birkhäuser, Boston, 2009. MR Zbl

[Deligne 1989] P. Deligne, "Le groupe fondamental de la droite projective moins trois points", pp. 79–297 in *Galois groups over* $\mathbb{Q}$ (Berkeley, 1987), edited by Y. Ihara et al., Math. Sci. Res. Inst. Publ. **16**, Springer, 1989. MR Zbl

[Enriquez and Etingof 2018] B. Enriquez and P. Etingof, "A Tannakian interpretation of the elliptic infinitesimal braid Lie algebras", *Algebr. Represent. Theory* **21**:5 (2018), 943–1002. MR Zbl

[Hain 1986] R. M. Hain, "On a generalization of Hilbert's 21st problem", *Ann. Sci. École Norm. Sup.* (4) **19**:4 (1986), 609–627. MR Zbl

[Hain 1987] R. M. Hain, "The de Rham homotopy theory of complex algebraic varieties, II", *K-Theory* **1**:5 (1987), 481–497. MR Zbl

[Hain 2011] R. Hain, "Lectures on moduli spaces of elliptic curves", pp. 95–166 in *Transformation groups and moduli spaces of curves* (Hangzhou, 2008), edited by L. Ji and S.-T. Yau, Adv. Lect. Math. **16**, Int. Press, Somerville, MA, 2011. MR Zbl

[Hain 2013] R. Hain, "Notes on the universal elliptic KZB equation", 2013. To appear in *Pure Appl. Math. Q.* arXiv

[Hain and Matsumoto 2018] R. Hain and M. Matsumoto, "Universal mixed elliptic motives", *J. Inst. Math. Jussieu* (online publication April 2018).

[Katz and Mazur 1985] N. M. Katz and B. Mazur, *Arithmetic moduli of elliptic curves*, Ann. Math. Stud. **108**, Princeton Univ. Press, 1985. MR Zbl

[Levin and Racinet 2007] A. Levin and G. Racinet, "Towards multiple elliptic polylogarithms", preprint, 2007. arXiv

[Silverman 1994] J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Grad. Texts in Math. **151**, Springer, 1994. MR Zbl

[Weil 1976] A. Weil, *Elliptic functions according to Eisenstein and Kronecker*, Ergebnisse der Mathematik (3) **88**, Springer, 1976. MR Zbl

[Zagier 1991] D. Zagier, "Periods of modular forms and Jacobi theta functions", *Invent. Math.* **104**:3 (1991), 449–465. MR Zbl

Communicated by Martin Olsson
Received 2018-03-27 Revised 2019-01-23 Accepted 2019-07-12

ma.luo@maths.ox.ac.uk *University of Oxford, United Kingdom*

ALGEBRA AND NUMBER THEORY 13:10 (2019)
dx.doi.org/10.2140/ant.2019.13.2277

Moments of random multiplicative functions, II: High moments

Adam J Harper

We determine the order of magnitude of $\mathbb{E}\left|\sum_{n\le x} f(n)\right|^{2q}$ up to factors of size $e^{O(q^2)}$, where $f(n)$ is a Steinhaus or Rademacher random multiplicative function, for all real $1\le q\le c\log x/\log\log x$.

In the Steinhaus case, we show that $\mathbb{E}\left|\sum_{n\le x} f(n)\right|^{2q} = e^{O(q^2)} x^q (\log x/(q\log(2q)))^{(q-1)^2}$ on this whole range. In the Rademacher case, we find a transition in the behavior of the moments when $q\approx(1+\sqrt{5})/2$, where the size starts to be dominated by "orthogonal" rather than "unitary" behavior. We also deduce some consequences for the large deviations of $\sum_{n\le x} f(n)$.

The proofs use various tools, including hypercontractive inequalities, to connect $\mathbb{E}\left|\sum_{n\le x} f(n)\right|^{2q}$ with the q-th moment of an Euler product integral. When q is large, it is then fairly easy to analyze this integral. When q is close to 1 the analysis seems to require subtler arguments, including Doob's L^p maximal inequality for martingales.

1. Introduction

In this sequence of papers, we are interested in the moments $\mathbb{E}\left|\sum_{n\le x} f(n)\right|^{2q}$ of random multiplicative functions $f(n)$.

We consider two different models for $f(n)$, a *Steinhaus random multiplicative function* and a *Rademacher random multiplicative function*. We obtain a Steinhaus random multiplicative function by letting $(f(p))_{p \text{ prime}}$ be a sequence of independent Steinhaus random variables (i.e., distributed uniformly on the unit circle $\{|z|=1\}$), and then setting $f(n):=\prod_{p^a \,\|\, n} f(p)^a$ for all natural numbers n, where $p^a \,\|\, n$ means that p^a is the highest power of the prime p that divides n. We obtain a Rademacher random multiplicative function by letting $(f(p))_{p \text{ prime}}$ be independent Rademacher random variables (i.e., taking values ± 1 with probability $\frac{1}{2}$ each), and then setting $f(n):=\prod_{p\,|\,n} f(p)$ for all squarefree n, and $f(n)=0$ when n is not squarefree.

Random multiplicative functions have attracted quite a lot of attention as models for functions of number theoretic interest: for example, Rademacher random multiplicative functions were introduced by Wintner [1944] as a model for the Möbius function $\mu(n)$. There are also probabilistic and analytic

When this work was started, the author was supported by a research fellowship at Jesus College, Cambridge. The work continued while the author was in residence at the Mathematical Sciences Research Institute in Berkeley, California (supported by the National Science Foundation under Grant No. DMS-1440140), during the Spring 2017 semester.
MSC2010: primary 11N56; secondary 11K65, 11L40.
Keywords: random multiplicative functions, random Euler products, moments, orthogonal behavior, unitary behavior, martingales.

motivations for studying them, see Saksman and Seip's open problems paper [2016], for example. The introduction to the previous paper [Harper 2017] in this sequence contains a more extensive discussion of some of these connections.

Harper [2017] showed that for Steinhaus or Rademacher random multiplicative $f(n)$, for all large x we have

$$\mathbb{E}\Big|\sum_{n\le x} f(n)\Big|^{2q} \asymp \left(\frac{x}{1+(1-q)\sqrt{\log\log x}}\right)^q \quad \forall 0\le q\le 1.$$

In particular, taking $q=\frac{1}{2}$ this implies that $\mathbb{E}\big|\sum_{n\le x} f(n)\big| \asymp \sqrt{x}/(\log\log x)^{1/4}$, which proved a conjecture of Helson [2010] that the first absolute moment should be $o(\sqrt{x})$.

Our goal here is to investigate the case where $q\ge 1$. When $q\in\mathbb{N}$ is fixed, one can expand the $2q$-th power and reduce the calculation of $\mathbb{E}\big|\sum_{n\le x} f(n)\big|^{2q}$ to a number theoretic counting problem. For example, in the Steinhaus case one has

$$\mathbb{E}\Big|\sum_{n\le x} f(n)\Big|^{2q} = \#\left\{n_1,\dots,n_{2q}\le x : \prod_{i=1}^{q} n_i = \prod_{i=q+1}^{2q} n_i\right\}.$$

Starting from this, one can obtain an asymptotic for the moment as $x\to\infty$, which was carried out by Harper, Nikeghbali and Radziwiłł [Harper et al. 2015], and also independently by Heap and Lindqvist [2016], and (in the Steinhaus case) in unpublished work of Granville and Soundararajan. The result is that, for fixed $q\in\mathbb{N}$ and Steinhaus random multiplicative $f(n)$, one has

$$\mathbb{E}\Big|\sum_{n\le x} f(n)\Big|^{2q} \sim C_{\mathrm{St}}(q)x^q \log^{(q-1)^2} x \quad \text{as } x\to\infty, \tag{1-1}$$

where the constant $C_{\mathrm{St}}(q)$ satisfies $C_{\mathrm{St}}(q)=e^{-q^2\log q-q^2\log\log q+O(q^2)}$ for large q. For Rademacher random multiplicative $f(n)$, when $q=1$ we have that $\mathbb{E}\big|\sum_{n\le x} f(n)\big|^2=\sum_{n\le x,n \text{ squarefree}} 1\sim(6/\pi^2)x$, and for fixed integer $q\ge 2$ we have

$$\mathbb{E}\Big|\sum_{n\le x} f(n)\Big|^{2q} \sim C_{\mathrm{Rad}}(q)x^q \log^{q(2q-3)} x \quad \text{as } x\to\infty,$$

where the constant $C_{\mathrm{Rad}}(q)$ satisfies $C_{\mathrm{Rad}}(q)=e^{-2q^2\log q-2q^2\log\log q+O(q^2)}$ for large q. As described in [Harper et al. 2015; Heap and Lindqvist 2016], we actually have much more precise information about the constants $C_{\mathrm{St}}(q)$, $C_{\mathrm{Rad}}(q)$ (for example they factor into explicit "arithmetic" and "geometric" parts), but this will not be important for our purposes here.

We would like to have information about $\mathbb{E}\big|\sum_{n\le x} f(n)\big|^{2q}$ when $q\ge 1$ is not necessarily integral, and that allows q to vary as a function of x rather than being fixed.

Regarding uniformity in q, Theorem 4.1 of [Granville and Soundararajan 2001] implies that for Steinhaus random multiplicative $f(n)$, and uniformly for all large x and integers $q\ge 1$ such that $q^{eq}\le x$, we have

$$e^{-q^2\log q-q^2\log\log(2q)}\left(\log\left(\frac{\log x}{q\log 2q}\right)\right)^{-O(q^2)}\le\frac{\mathbb{E}\left|\sum_{n\le x}f(n)\right|^{2q}}{x^q\log^{(q-1)^2}x}\le e^{-q^2\log q+O(q^2)}.$$

This range of q is essentially the largest on which one could expect a result of a similar shape to (1-1). Indeed, if $q\ge A\log x/\log\log x$ for some $A\ge 1$ (say) then we have

$$e^{-q^2\log q-q^2\log\log(2q)}x^q\log^{(q-1)^2}x\le((1+o(1))A)^{-q^2}x^q,$$

which becomes incompatible with the lower bound $\mathbb{E}\left|\sum_{n\le x}f(n)\right|^{2q}\ge\left(\mathbb{E}\left|\sum_{n\le x}f(n)\right|^2\right)^q=\lfloor x\rfloor^q$ coming from Hölder's inequality.[1] But the bounds of Granville and Soundararajan are imperfect, as the upper bound doesn't include the factor $e^{-q^2\log\log(2q)}$ that we expect to appear, and the lower bound features the extraneous factor $(\log(\log x/(q\log 2q)))^{-O(q^2)}$. They also remain restricted to *integer* q. There are various other results in the literature that study the Steinhaus moments $\mathbb{E}\left|\sum_{n\le x}f(n)\right|^{2q}$, and variants of them, for integer q, especially for small integers where one can try to obtain lower order terms in the known asymptotics. See e.g., the preprint of Shi and Weber [2016]. However, the author is not aware of any work giving sharp moment bounds for noninteger q, nor improving the dependence on q in Granville and Soundararajan's bounds [2001] for the large integer case.

We shall prove the following uniform estimate for all *real* q.

Theorem 1.1. *There exists a small absolute constant $c>0$ such that the following is true. If $f(n)$ is a Steinhaus random multiplicative function, then uniformly for all large x and real $1\le q\le c\log x/(\log\log x)$ we have*

$$\mathbb{E}\left|\sum_{n\le x}f(n)\right|^{2q}=e^{-q^2\log q-q^2\log\log(2q)+O(q^2)}x^q\log^{(q-1)^2}x.$$

To avoid any confusion, we restate this first result more explicitly: on the stated range of q and x, we always have

$$e^{-q^2\log q-q^2\log\log(2q)-Cq^2}\le\frac{\mathbb{E}\left|\sum_{n\le x}f(n)\right|^{2q}}{x^q\log^{(q-1)^2}x}\le e^{-q^2\log q-q^2\log\log(2q)+Cq^2},$$

for a certain absolute constant C. We do *not* know how to prove an asymptotic like (1-1) when q is not a fixed natural number.

[1] In this paper we are not particularly concerned with the case where $q\ge\log x/\log\log x$, but for completeness we make a few indicative remarks. Section 6 of Granville and Soundararajan [2001] contains various results on this range of q. Setting $v=\log(2q(\log q)/\log x)\gg 1$, and redoing the calculations on page 2293 with the Rankin shift $1+q/\log x$ replaced by $1+v/\log(q\log x)$ and with q^2-smooth numbers replaced by $q\log x$-smooth numbers, one can show that $\mathbb{E}\left|\sum_{n\le x}f(n)\right|^{2q}\le x^{q(1+v/\log(q\log x)+o(1))}$ uniformly for $q\ge\log x/\log\log x$. In particular, if $q=\log^{1+a}x$ for any fixed $a\ge 0$ then we have $\mathbb{E}\left|\sum_{n\le x}f(n)\right|^{2q}\le x^{q(1+a/(a+2)+o(1))}$. By only considering the contribution to the expectation from the event that $f(p)$ is very close to 1 for all primes $p\le q\log x/\log\log x=\log^{2+a}x/\log\log x$, one can obtain a comparable lower bound for $\mathbb{E}\left|\sum_{n\le x}f(n)\right|^{2q}$ (as in Corollary 6.3 of Granville and Soundararajan [2001]).

In the Rademacher case, even conjecturally the behavior of $\mathbb{E}\big|\sum_{n\le x} f(n)\big|^{2q}$ is perhaps not obvious. On a wide range of real $q \ge 2$, we might expect that

$$\mathbb{E}\Big|\sum_{n\le x} f(n)\Big|^{2q} = e^{-2q^2\log q - 2q^2\log\log(2q) + O(q^2)} x^q \log^{q(2q-3)} x$$

as in the known asymptotics. But this certainly cannot be the answer for all $1 \le q \le 2$, since on some of that range the exponent $q(2q-3)$ of the logarithm would be negative. (And, by Hölder's inequality, we must at least have $\mathbb{E}\big|\sum_{n\le x} f(n)\big|^{2q} \ge \big(\mathbb{E}\big|\sum_{n\le x} f(n)\big|^2\big)^q \gg x^q$.)

Theorem 1.2. *Let $q_0 = (1+\sqrt{5})/2 \approx 1.618$. There exists a small absolute constant $c > 0$ such that the following is true. If $f(n)$ is a Rademacher random multiplicative function, then uniformly for all large x and real $1 \le q \le c\log x/\log\log x$ we have*

$$\mathbb{E}\Big|\sum_{n\le x} f(n)\Big|^{2q} = e^{-2q^2\log q - 2q^2\log\log(2q) + O(q^2)} \Big(1 + \min\Big\{\log\log x, \tfrac{1}{|q-q_0|}\Big\}\Big) x^q \log^{\max\{(q-1)^2, q(2q-3)\}} x.$$

With hindsight, the exponent of $\log x$ we obtain in Theorem 1.2 is perhaps quite natural, since one doesn't expect slower growth in the Rademacher than the Steinhaus case (where there is "more room" for the complex valued random variables to cancel), and we expect $q(2q-3)$ to be the correct exponent eventually. Notice that the golden ratio q_0 is the value at which $q(2q-3)$ becomes larger than $(q-1)^2$. But the additional factor $\min\{\log\log x, 1/|q-q_0|\}$ that appears for q close to q_0 seems genuinely unexpected, and hard to understand except through an inspection of the proof of the theorem.

Next we shall discuss the proofs. Once q is moderately large, namely when $q \ge \log\log x$, we can prove the upper bounds in Theorems 1.1 and 1.2 by fairly simple arguments. See Section 3. This is because, for such q, terms like $\log^{O(q)} x$ can be absorbed into the factor $e^{O(q^2)}$ in our theorems, so we can afford to use simple techniques that are a bit wasteful (e.g., involving Hölder's inequality to reduce to the case of integer q) to reduce matters to a counting problem. Then Rankin's trick is almost sufficient to perform the relevant counts. To obtain the terms $e^{-q^2\log\log(2q)}$ and $e^{-2q^2\log\log(2q)}$ in the theorems, we use Rankin's trick along with a slightly more careful treatment of small prime factors.

Our main work is to prove Theorems 1.1 and 1.2 for $1 \le q \le \log\log x$, and also the lower bounds for larger q. Let $F(s) = \sum_{n=1,\, p\,|\,n \Rightarrow p\le x}^{\infty} f(n)/n^s$ denote the Dirichlet series corresponding to $f(n)$, on x-smooth numbers (i.e., numbers with all their prime factors $\le x$). We can also write $F(s)$ as an Euler product, namely $F(s) = \prod_{p\le x}(1 - f(p)/p^s)^{-1}$ in the Steinhaus case and $F(s) = \prod_{p\le x}(1 + f(p)/p^s)$ in the Rademacher case. In the author's treatment [Harper 2017] of low moments, the first step was to show (roughly) that $\mathbb{E}\big|\sum_{n\le x} f(n)\big|^{2q} \approx x^q\,\mathbb{E}\big(\frac{1}{\log x}\int_{-1/2}^{1/2} \big|F\big(\tfrac12 + it\big)\big|^2 dt\big)^q$ when $\frac23 \le q \le 1$. Similarly, our first step here is to show that

$$\mathbb{E}\Big|\sum_{n\le x} f(n)\Big|^{2q} \approx e^{O(q^2)} x^q\,\mathbb{E}\Big(\frac{1}{\log x}\int_{-1/2}^{1/2} \Big|F\Big(\tfrac12 + \tfrac{q}{\log x} + it\Big)\Big|^2 dt\Big)^q. \tag{1-2}$$

Note the shift by $q/\log x$ in the integral, which is analogous to the use of Rankin's trick in our elementary upper bound argument for $q \geq \log\log x$. The basic strategy for proving something like (1-2) is the same as in [Harper 2017], namely conditioning on the behavior of $f(n)$ on smaller primes; using fairly standard moment inequalities, like Khintchine's inequality, to show the conditional expectation behaves like a power of a mean square average; and using Parseval's identity to relate the mean square to an integral average of the Euler product. In [Harper 2017] one could bound terms by using Hölder's inequality to pass to the second moment, whereas here we need suitable rough bounds for high moments. These are supplied by a pair of hypercontractive inequalities, see Probability Result 2.3 in Section 2. Applying the hypercontractive inequalities introduces various divisor functions $d_{\lceil q \rceil}(n)$, $d_{2\lceil q \rceil - 1}(n)$ into our calculations, requiring a bit more number theoretic work as compared with the low moments argument of [Harper 2017]. We refer to the beginning of Section 4 for a rigorous formulation of (1-2), and more technical comparison of this part of the argument with the low moments case [Harper 2017].

Next, we observe that the right-hand side of (1-2) is

$$\approx e^{O(q^2)} x^q \mathbb{E}\left(\frac{1}{\log^2 x} \sum_{|n| \leq (\log x)/2} \left| F\left(\tfrac{1}{2} + \tfrac{q}{\log x} + i\frac{n}{\log x}\right)\right|^2 \right)^q, \tag{1-3}$$

since heuristically the value of $\left|F\left(\frac{1}{2} + \frac{q}{\log x} + it\right)\right|$ doesn't change much on t intervals of length $1/\log x$. One can obtain rigorous statements of this kind using Hölder's inequality in the upper bound arguments, and Jensen's inequality in the lower bound arguments, see Sections 5 and 6. Now we can see heuristically why Theorems 1.1 and 1.2 might hold. In the Steinhaus case, the Euler product $F(s)$ behaves on average like an L-function from a *unitary* family, and then since we have $q \geq 1$ (and very differently than in the low moments case [Harper 2017]) the sum over n essentially gives us $\log x$ independent tries at obtaining a large value of $F(s)$. So the right-hand side of (1-3) is $\approx e^{O(q^2)} x^q \frac{1}{\log^{2q} x} \log x \mathbb{E}\left|F\left(\frac{1}{2} + \frac{q}{\log x}\right)\right|^{2q} \approx e^{O(q^2)} x^q \frac{1}{\log^{2q-1} x}\left(\frac{\log x}{q\log(2q)}\right)^{q^2}$, as in Theorem 1.1. In the Rademacher case, $F\left(\frac{1}{2} + \frac{q}{\log x} + it\right)$ behaves like an L-function from an *orthogonal* family when $t \approx 0$, and like an L-function from a unitary family[2] when $t \approx 1$. Thus, thanks to those $(\log x)/4 \leq |n| \leq (\log x)/2$ (say) we get a contribution $e^{O(q^2)} x^q \frac{1}{\log^{2q-1} x}\left(\frac{\log x}{q\log(2q)}\right)^{q^2}$ to the right-hand side of (1-3), and thanks to the $n = 0$ term we get a contribution $\approx e^{O(q^2)} x^q \frac{1}{\log^{2q} x} \mathbb{E}\left|F\left(\frac{1}{2} + \frac{q}{\log x}\right)\right|^{2q} \approx e^{O(q^2)} x^q \frac{1}{\log^{2q} x}\left(\frac{\log x}{q\log(2q)}\right)^{2q^2 - q}$. The factor $(1 + \min\{\log\log x, 1/|q - q_0|\})$ in Theorem 1.2 arises because of the contribution from intermediate values of n.

To prove the lower bounds in Theorems 1.1 and 1.2 rigorously, as we do in Section 6, roughly speaking it suffices to note that (1-3) is $\geq e^{O(q^2)} x^q \frac{1}{\log^{2q} x} \mathbb{E} \sum_{|n| \leq (\log x)/2} \left|F\left(\frac{1}{2} + \frac{q}{\log x} + i\frac{n}{\log x}\right)\right|^{2q}$, and then compute $\mathbb{E}\left|F\left(\frac{1}{2} + \frac{q}{\log x} + i\frac{n}{\log x}\right)\right|^{2q}$. In practice the details are slightly more complicated because the precise version of (1-3) involves some other terms, including subtracted error terms that must be upper bounded. However,

[2] At first glance, one might expect $F\left(\frac{1}{2} + \frac{q}{\log x} + it\right)$ to behave like a *symplectic* L-function when $t \approx 0$, because averaging over Rademacher $f(n)$ models averaging over quadratic Dirichlet characters. The reason we actually have orthogonal behavior is because we restrict our sums $\sum_{n \leq x} f(n)$ to squarefree terms. For some other contexts where a transition from orthogonal/symplectic to unitary behavior arises, as for large t here, see the papers of Florea [2017], Keating and Odgers [2008], and Soundararajan and Young [2010], for example.

we can obtain suitable upper bounds from our main Section 5 argument for proving the upper bounds in Theorems 1.1 and 1.2.

To prove those upper bounds rigorously, we need to capture the fact that typically there will only be a few large terms in the sum over n in (1-3). When $q \geq 2$, a careful application of Hölder's inequality lets us bound (1-3) by estimating terms of the form $\mathbb{E}\big|F\big(\frac{1}{2}+\frac{q}{\log x}+i\frac{n}{\log x}\big)\big|^2\big|F\big(\frac{1}{2}+\frac{q}{\log x}+i\frac{m}{\log x}\big)\big|^{2(q-1)}$. These decrease in size quite rapidly as $|m-n|$ becomes large (and, in the Rademacher case, as $|m|$, $|n|$ become large), because the parts of the two Euler products over primes $> x^{1/|m-n|}$ become decorrelated rather than reinforcing one another. This indeed says that one doesn't expect large contributions from many different m, n. When $1 < q < 2$, such a direct argument doesn't seem to succeed, so we need a more subtle approach. The rough idea is to treat parts of the Euler products over "small" and "large" primes differently, so after a (different) careful application of Hölder's inequality, one is led to expectations where different parts of the Euler product appear to different exponents, to maximize the decorrelation we capture. The most difficult situation is where q is very close to 1 (i.e., $q = 1+o(1)$ as $x \to \infty$). To handle this without picking up any terms that blow up as q approaches 1, we use a martingale maximal inequality (see Probability Result 2.5 in Section 2) that essentially lets us maximize over several different splittings of the Euler product simultaneously.

As just described, we go to quite a lot of trouble to prove Theorems 1.1 and 1.2 when q is just a little larger than 1. It is satisfying to have a uniform result (and a method capable of proving one), but in addition this range of q turns out to be relevant for deducing the following corollary.

Corollary 1.3. *Let x be large, and let $f(n)$ be a Steinhaus or Rademacher random multiplicative function. For all $2 \leq \lambda \leq \sqrt{\log x}$, say, we have*

$$\mathbb{P}\bigg(\bigg|\sum_{n\leq x} f(n)\bigg| \geq \lambda\sqrt{x}\bigg) \ll \frac{1}{\lambda^2}e^{-(\log^2\lambda)/\log\log x}.$$

Proof of Corollary 1.3. For any $1 \leq q \leq \frac{3}{2}$, say, Theorems 1.1 and 1.2 imply that

$$\mathbb{P}\bigg(\bigg|\sum_{n\leq x} f(n)\bigg| \geq \lambda\sqrt{x}\bigg) \leq \frac{\mathbb{E}\big|\sum_{n\leq x} f(n)\big|^{2q}}{(\lambda\sqrt{x})^{2q}} \ll \frac{\log^{(q-1)^2} x}{\lambda^{2q}} = \frac{1}{\lambda^2}e^{(q-1)^2\log\log x-2(q-1)\log\lambda}.$$

Calculus implies that the right-hand side is minimized if we choose $q-1 = \frac{\log\lambda}{\log\log x}$, and inserting this choice proves Corollary 1.3. □

In the paper [Harper 2017] on low moments, by considering $\mathbb{E}\big|\sum_{n\leq x} f(n)\big|^{2q}$ with q a little smaller than 1 the author showed that $\mathbb{P}\big(\big|\sum_{n\leq x} f(n)\big| \geq z\sqrt{x}/(\log\log x)^{1/4}\big) \ll \min\{\log z, \sqrt{\log\log x}\}/z^2$ for all $z \geq 2$. Corollary 1.3 is weaker than this when $\lambda \leq e^{\sqrt{\log\log x}}$, but stronger for larger λ. In [loc. cit.] the author also showed (see Corollary 2 there, and the subsequent discussion) that $\mathbb{P}\big(\big|\sum_{n\leq x} f(n)\big| \geq z\sqrt{x}/(\log\log x)^{1/4}\big) \gg e^{-(\log^2 z)/\log\log x}/z^2(\log\log x)^{O(1)}$ on a wide range of z. Together all these results give a fairly complete description of the tail behavior of $\sum_{n\leq x} f(n)$, up to factors $(\log\log x)^{O(1)}$.

We end this introduction with a few remarks on other possible approaches to Theorems 1.1 and 1.2, and connections with the wider literature.

The quantity $\frac{1}{\log x}\int_{-1/2}^{1/2}\left|F\left(\frac{1}{2}+\frac{q}{\log x}+it\right)\right|^2 dt$ in (1-2) is closely related to (the total mass of a truncation of) a probabilistic object called *critical multiplicative chaos*. This connection is discussed extensively in the introduction to the low moments paper [Harper 2017], since in that case the techniques for analyzing $\mathbb{E}\left(\frac{1}{\log x}\int_{-1/2}^{1/2}\left|F\left(\frac{1}{2}+\frac{q}{\log x}+it\right)\right|^2 dt\right)^q$ are heavily motivated by ideas from the multiplicative chaos literature. When $q > 1$ the analogous problem does not seem to have been investigated for critical multiplicative chaos, since the q-th moment of the integral will diverge as $x \to \infty$ and this seems to be all the information that was wanted in that case (where the usual interest is in letting $x \to \infty$ and obtaining a limiting measure whose properties can be investigated). Theorems 1.1 and 1.2 show very different behavior in the Steinhaus and Rademacher cases when q is large, whereas in the usual problems of multiplicative chaos one finds rather universal behavior (and indeed the Steinhaus and Rademacher moments are of the same order when $q \le 1$).

Assuming the generalized Riemann hypothesis for Dirichlet L-functions, Munsch [2017] proved almost sharp upper bounds for the $2k$-th moment of theta functions $\theta(1,\chi)$ as the character χ varies over nonprincipal Dirichlet characters mod q, for each fixed $k \in \mathbb{N}$. He did this by writing $\theta(1,\chi)$ as a Perron integral involving the L-function $L(s,\chi)$, and then expanding the $2k$-th power and bounding the averages of products $\prod_{j=1}^{2k}\left|L\left(\frac{1}{2}+it_j,\chi\right)\right|$ that emerge. This is interesting here because for even characters χ, $\theta(1,\chi)$ behaves roughly like $\sum_{n\le\sqrt{q}}\chi(n)$, which is modeled by the sum $\sum_{n\le\sqrt{q}} f(n)$ of a Steinhaus random multiplicative function. In our case, using Perron's formula we have

$$\mathbb{E}\left|\sum_{n\le x} f(n)\right|^{2q} \approx \mathbb{E}\left|\frac{1}{2\pi}\int_{-\sqrt{x}}^{\sqrt{x}} F\left(\tfrac{1}{2}+\tfrac{q}{\log x}+it\right)\frac{x^{1/2+q/\log x+it}}{1/2+q/\log x+it}\,dt\right|^{2q}$$

$$\le x^q e^{O(q^2)}\mathbb{E}\left(\int_{-\sqrt{x}}^{\sqrt{x}}\left|F\left(\tfrac{1}{2}+\tfrac{q}{\log x}+it\right)\right|\frac{dt}{|1/2+q/\log x+it|}\right)^{2q},$$

say. We already have asymptotics for $\mathbb{E}\left|\sum_{n\le x} f(n)\right|^{2q}$ for fixed $q \in \mathbb{N}$, but we might hope to get an alternative proof of sharp upper bounds for $q \notin \mathbb{N}$ by using Hölder's inequality in some way. A direct application, producing a term $\left|F\left(\frac{1}{2}+\frac{q}{\log x}+it\right)\right|^{2q}$, cannot give sharp bounds because it doesn't recognize that the size of the expectation will be dominated by the integral of $F\left(\frac{1}{2}+\frac{q}{\log x}+it\right)$ over a very short (random) t interval. To detect this, one could pull out a few (say d) copies of the bracket before applying Hölder's inequality to the remaining ones. This would produce a multiple integral of terms of the form $\mathbb{E}\left(\prod_{j=1}^{d}\left|F\left(\frac{1}{2}+\frac{q}{\log x}+it_j\right)\right|\right)\left|F\left(\frac{1}{2}+\frac{q}{\log x}+iu\right)\right|^{2q-d}$, and the biggest contribution comes when all of the t_j are approximately equal to u, so indeed we would capture the localization of the largest contributions. Based on a few rough calculations, it appears this alternative method can prove sharp upper bounds if we take $d = 3$ (we need to pull out enough terms to adequately detect the localization), and if $q \ge 5$, say. But for smaller q this kind of argument doesn't seem operable to prove sharp bounds, indeed one has already lost too much information in applying the triangle inequality to the Perron integral. Nevertheless, it might permit a relatively straightforward extension of Munsch's results [2017] to noninteger $k \ge 5$.

A standard strategy for proving lower bounds is to calculate

$$\mathbb{E}\Big(\sum_{n\le x} f(n)\Big) R_{x,q}(f) \quad \text{and} \quad \mathbb{E}|R_{x,q}(f)|^{2q/(2q-1)},$$

where $R_{x,q}(f)$ is some function that is chosen as a proxy for $\big(\sum_{n\le x} f(n)\big)^{2q-1}$ that is easier to understand. Then Hölder's inequality gives

$$\mathbb{E}\Big|\sum_{n\le x} f(n)\Big|^{2q} \ge \frac{\big|\mathbb{E}\big(\sum_{n\le x} f(n)\big)R_{x,q}(f)\big|^{2q}}{(\mathbb{E}|R_{x,q}(f)|^{2q/(2q-1)})^{2q-1}}.$$

If we can estimate the expectations in the numerator and denominator, and $R_{x,q}(f)$ is well chosen so that both of them do behave like $\mathbb{E}\big|\sum_{n\le x} f(n)\big|^{2q}$ (up to scaling factors that would cancel out), then one obtains a sharp lower bound for the $2q$-th moment. Munsch and Shparlinski [2016] proved sharp lower bounds for the $2k$-th moments of theta functions $\theta(1,\chi)$, for fixed $k\in\mathbb{N}$, by implementing this strategy with a power of a short character sum chosen as the "proxy" object. Our analysis shows that for Rademacher random multiplicative functions, we can imagine heuristically that $\big|\sum_{n\le x} f(n)\big| \approx \frac{\sqrt{x}}{\log x}\big|F\big(\frac{1}{2}+\frac{q}{\log x}\big)\big|$ (when studying $2q$-th moments with $q>q_0$). Motivated by this, we could try taking $R_{x,q}(f)=\big|F\big(\frac{1}{2}+\frac{q}{\log x}\big)\big|^{2q-1}$, or perhaps a small variant of this where primes smaller than $q^{O(1)}$ are excluded from the Euler product. In the Rademacher case, rough calculations suggest this will indeed yield the lower bound $\mathbb{E}\big|\sum_{n\le x} f(n)\big|^{2q}\ge e^{O(q^2)}x^q(\log x/(q\log(2q)))^{q(2q-3)}$, which is sharp when $q>q_0$. For smaller q, and in the Steinhaus case, our analysis suggests taking $R_{x,q}(f)=\sum_{|m|\le\log x}\big|F\big(\frac{1}{2}+\frac{q}{\log x}+i\frac{m}{\log x}\big)\big|^{2q-1}$. This choice actually won't quite work, but rough calculations suggest that comparing $\mathbb{E}\big|\sum_{n\le x} f(n)\big|^2\sum_{|m|\le\log x}\big|F\big(\frac{1}{2}+\frac{q}{\log x}+i\frac{m}{\log x}\big)\big|^{2(q-1)}$ and $\mathbb{E}\big(\sum_{|m|\le\log x}\big|F\big(\frac{1}{2}+\frac{q}{\log x}+i\frac{m}{\log x}\big)\big|^{2(q-1)}\big)^{q/(q-1)}$ will yield sharp lower bounds for $\mathbb{E}\big|\sum_{n\le x} f(n)\big|^{2q}$. This does not seem simpler than our original proofs of the lower bounds in Theorems 1.1 and 1.2, however.

Notation and references. We will say a number n is y-smooth if all prime factors of n are $\le y$. We will generally use p to denote primes. Unless mentioned otherwise, the letters c, C will denote positive constants, c usually being a small constant and C a large one. We write $f(x)=O(g(x))$ and $f(x)\ll g(x)$, both of which mean that there exists C such that $|f(x)|\le Cg(x)$, for all x. Sometimes this notation will be adorned with a subscript parameter (e.g., $O_\epsilon(\cdot)$ and $\ll_\delta$), meaning that the implied constant C is allowed to depend on that parameter. We write $f(x)\asymp g(x)$ to mean that $g(x)\ll f(x)\ll g(x)$, in other words that $cg(x)\le|f(x)|\le Cg(x)$ for some c, C, for all x.

The books of Gut [2013] and of Montgomery and Vaughan [2007] may be consulted as excellent general references for probabilistic and number theoretic background for this paper.

2. Preliminary results

Random Euler products. We begin with some "two point" estimates for the expectation of the 2α-th power of a random Euler product, multiplied by the 2β-th power of an imaginary shift of that product.

These estimates, and small variants of them, will be basic tools throughout our work. The calculations are closely related to computations of shifted moments of L-functions, as in the papers of Chandee [2011] and of Soundararajan and Young [2010], for example.

Euler Product Result 2.1. *If f is a Steinhaus random multiplicative function, then for any real $\alpha, \beta \geq 0$, any real $100(1+\max\{\alpha^2, \beta^2\}) \leq x \leq y$, and any real $\sigma \geq -1/\log y$ and t, we have*

$$\mathbb{E} \prod_{x<p\leq y} \left|1-\frac{f(p)}{p^{1/2+\sigma}}\right|^{-2\alpha} \left|1-\frac{f(p)}{p^{1/2+\sigma+it}}\right|^{-2\beta} = \exp\left\{ \sum_{x<p\leq y} \frac{\alpha^2+\beta^2+2\alpha\beta\cos(t\log p)}{p^{1+2\sigma}} + O\left(\frac{\max\{\alpha, \beta, \alpha^3, \beta^3\}}{\sqrt{x}\log x}\right)\right\}.$$

If we also have $\sigma \leq 1/\log y$, then the above is

$$= e^{O(\max\{\alpha,\beta,\alpha^2,\beta^2\}(1+|t|/\log^{100} x))} \left(\frac{\log y}{\log x}\right)^{\alpha^2+\beta^2} \left(1+\min\left\{\frac{\log y}{\log x}, \frac{1}{|t|\log x}\right\}\right)^{2\alpha\beta}.$$

In particular, for any real $\alpha \geq 0$, any real $100(1+\alpha^2) \leq x \leq y$, and any real $\sigma \geq -1/\log y$, we have

$$\mathbb{E} \prod_{x<p\leq y} \left|1-\frac{f(p)}{p^{1/2+\sigma}}\right|^{-2\alpha} = \exp\left\{ \sum_{x<p\leq y} \frac{\alpha^2}{p^{1+2\sigma}} + O\left(\frac{\max\{\alpha, \alpha^3\}}{\sqrt{x}\log x}\right)\right\},$$

and if $\sigma \leq 1/\log y$ as well then this is $= e^{O(\max\{\alpha,\alpha^2\})}(\log y/\log x)^{\alpha^2}$.

Proof of Euler Product Result 2.1. For concision in writing the proof, let us temporarily set $M = M(\alpha, \beta) := \max\{\alpha, \beta, \alpha^3, \beta^3\}$.

Firstly, using the Taylor expansion of the logarithm we may rewrite

$$\begin{aligned} &\left|1-\frac{f(p)}{p^{1/2+\sigma}}\right|^{-2\alpha} \left|1-\frac{f(p)}{p^{1/2+\sigma+it}}\right|^{-2\beta} \\ &= \exp\left\{-2\alpha\Re\log\left(1-\frac{f(p)}{p^{1/2+\sigma}}\right) - 2\beta\Re\log\left(1-\frac{f(p)}{p^{1/2+\sigma+it}}\right)\right\} \\ &= \exp\left\{\frac{2\alpha\Re f(p)}{p^{1/2+\sigma}} + \frac{\alpha\Re f(p)^2}{p^{1+2\sigma}} + \frac{2\beta\Re f(p)p^{-it}}{p^{1/2+\sigma}} + \frac{\beta\Re f(p)^2 p^{-2it}}{p^{1+2\sigma}} + O\left(\frac{\max\{\alpha, \beta\}}{p^{3/2+3\sigma}}\right)\right\}. \end{aligned}$$

Next, if $y \geq p > x \geq 100\max\{\alpha^2, \beta^2\}$ then every term in the exponential here has size at most $2\max\{\alpha, \beta\}/p^{1/2+\sigma} = 2\max\{\alpha, \beta\}e^{-\sigma\log p}/p^{1/2} \leq e/5$. Therefore we may apply the series expansion of the exponential function, finding the above is

$$= 1 + \frac{2(\alpha\Re f(p) + \beta\Re f(p)p^{-it})}{p^{1/2+\sigma}} + \frac{(\alpha\Re f(p)^2 + \beta\Re f(p)^2 p^{-2it})}{p^{1+2\sigma}} + \frac{2(\alpha\Re f(p) + \beta\Re f(p)p^{-it})^2}{p^{1+2\sigma}} + O\left(\frac{M}{p^{3/2+3\sigma}}\right).$$

Now taking expectations, by symmetry we have $\mathbb{E}\Re f(p) = \mathbb{E}\Re f(p)^2 = 0$, similarly for $\mathbb{E}\Re f(p)p^{-it}$ and $\mathbb{E}\Re f(p)^2 p^{-2it}$. A simple trigonometric calculation also shows that $\mathbb{E}(\Re f(p))^2 = \frac{1}{2}$, and similarly $\mathbb{E}\Re f(p)\Re f(p)p^{-it} = \cos(t\log p)/2$. So we get

$$\begin{aligned}
\mathbb{E}&\left|1-\frac{f(p)}{p^{1/2+\sigma}}\right|^{-2\alpha}\left|1-\frac{f(p)}{p^{1/2+\sigma+it}}\right|^{-2\beta} \\
&= 1+\frac{2\mathbb{E}(\alpha\Re f(p)+\beta\Re f(p)p^{-it})^2}{p^{1+2\sigma}} + O\left(\frac{M}{p^{3/2+3\sigma}}\right) \\
&= 1+\frac{2(\alpha^2\mathbb{E}(\Re f(p))^2 + 2\alpha\beta\mathbb{E}\Re f(p)\Re f(p)p^{-it} + \beta^2\mathbb{E}(\Re f(p)p^{-it})^2)}{p^{1+2\sigma}} + O\left(\frac{M}{p^{3/2+3\sigma}}\right) \\
&= 1+\frac{\alpha^2+\beta^2+2\alpha\beta\cos(t\log p)}{p^{1+2\sigma}} + O\left(\frac{M}{p^{3/2+3\sigma}}\right) \\
&= \exp\left\{\frac{\alpha^2+\beta^2+2\alpha\beta\cos(t\log p)}{p^{1+2\sigma}} + O\left(\frac{M}{p^{3/2+3\sigma}}\right)\right\}.
\end{aligned}$$

Combining the above calculation with the independence of f on distinct primes, and using that, for $p \le y$,

$$p^{3/2+\sigma} = e^{\sigma\log p}p^{3/2} \ge e^{-1}p^{3/2} \quad \text{and} \quad \sum_{p>x}\frac{1}{p^{3/2}} \ll \frac{1}{\sqrt{x}\log x},$$

we deduce that the quantity

$$\mathbb{E}\prod_{x<p\le y}\left|1-\frac{f(p)}{p^{1/2+\sigma}}\right|^{-2\alpha}\left|1-\frac{f(p)}{p^{1/2+\sigma+it}}\right|^{-2\beta}$$

in the statement of the result is

$$\begin{aligned}
&= \exp\left\{\sum_{x<p\le y}\left(\frac{\alpha^2+\beta^2+2\alpha\beta\cos(t\log p)}{p^{1+2\sigma}} + O\left(\frac{M}{p^{3/2+3\sigma}}\right)\right)\right\} \\
&= \exp\left\{\sum_{x<p\le y}\frac{\alpha^2+\beta^2+2\alpha\beta\cos(t\log p)}{p^{1+2\sigma}} + O\left(\frac{\max\{\alpha.\beta,\alpha^3,\beta^3\}}{\sqrt{x}\log x}\right)\right\}.
\end{aligned}$$

To deduce the second part of Euler Product Result 2.1, we can use standard estimates from prime number theory. Indeed, the Chebychev and Mertens estimates for sums over primes imply that

$$\begin{aligned}
\sum_{x<p\le y}\frac{\alpha^2+\beta^2}{p^{1+2\sigma}} &= (\alpha^2+\beta^2)\sum_{x<p\le y}\frac{1}{p} + (\alpha^2+\beta^2)\sum_{x<p\le y}\frac{e^{-2\sigma\log p}-1}{p} \\
&= (\alpha^2+\beta^2)\log\left(\frac{\log y}{\log x}\right) + O(\max\{\alpha^2,\beta^2\}),
\end{aligned}$$

using that $e^{-2\sigma\log p}-1 \ll |\sigma|\log p \ll \log p/\log y$ for $|\sigma| \le 1/\log y$. We may remove the nuisance factor $p^{2\sigma}$ from the sum $\sum_{x<p\le y}(2\alpha\beta\cos(t\log p))/p^{1+2\sigma}$ with the same error term. Then using the prime

number theorem in the form $\pi(z) := \#\{p \leq z : p \text{ prime}\} = \int_2^z 1/\log u\, du + O(z/(\log^{100} z))$, we have

$$\sum_{x<p\leq y} \frac{\cos(t\log p)}{p} = \int_x^y \frac{\cos(t\log z)}{z} d\pi(z)$$
$$= \int_x^y \frac{\cos(t\log z)}{z\log z} dz + O\left(\frac{1+|t|}{\log^{100} x}\right)$$
$$= \int_{\log x}^{\log y} \frac{\cos(tu)}{u} du + O\left(\frac{1+|t|}{\log^{100} x}\right).$$

Now if $|t|\log y \leq 1$, then the estimate $\cos(tu) = 1 + O((tu)^2)$ shows the integral is $\log\log y - \log\log x + O((t\log y)^2) = \log(\log y/\log x) + O(1)$. If instead we have $|t|\log x \leq 1$ but $|t|\log y > 1$, then we can evaluate the part of the integral with $u \leq 1/|t|$ using the estimate $\cos(tu) = 1 + O((tu)^2)$, and estimate the rest using integration by parts, yielding an overall estimate $\log(1/(|t|\log x)) + O(1)$. If $|t|\log x > 1$ then integration by parts shows the whole integral is $O(1)$. In any case, the second part of Euler Product Result 2.1 is proved.

The third part follows by setting $\beta = 0$ in the preceding statements. □

We will need a version of the above result for Rademacher random multiplicative functions. Unlike in the Steinhaus case, the distribution of $f(n)n^{-it}$ is not the same for all real t in the Rademacher case, so our general statement must allow two different imaginary shifts in our two Euler product factors.

Euler Product Result 2.2. *If f is a Rademacher random multiplicative function, then for any real $\alpha, \beta \geq 0$, any real $100(1+\max\{\alpha^2, \beta^2\}) \leq x \leq y$, and any real $\sigma \geq -1/\log y$ and t_1, t_2, we have*

$$\mathbb{E}\prod_{x<p\leq y}\left|1+\frac{f(p)}{p^{1/2+\sigma+it_1}}\right|^{2\alpha}\left|1+\frac{f(p)}{p^{1/2+\sigma+it_2}}\right|^{2\beta}$$
$$= \exp\Bigg\{\sum_{x<p\leq y}\frac{\alpha^2+\beta^2+(\alpha^2-\alpha)\cos(2t_1\log p)+(\beta^2-\beta)\cos(2t_2\log p)}{p^{1+2\sigma}}$$
$$+\sum_{x<p\leq y}\frac{2\alpha\beta(\cos((t_1+t_2)\log p)+\cos((t_1-t_2)\log p))}{p^{1+2\sigma}} + O\left(\frac{\max\{\alpha, \beta, \alpha^3, \beta^3\}}{\sqrt{x}\log x}\right)\Bigg\}.$$

If we also have $\sigma \leq 1/\log y$, then the above is

$$= e^{O(\max\{\alpha,\beta,\alpha^2,\beta^2\}(1+\frac{|t_1|+|t_2|}{\log^{100} x}))}\left(1+\min\left\{\frac{\log y}{\log x}, \frac{|t_1|^{-1}}{\log x}\right\}\right)^{\alpha^2-\alpha}\left(1+\min\left\{\frac{\log y}{\log x}, \frac{|t_2|^{-1}}{\log x}\right\}\right)^{\beta^2-\beta}$$
$$\cdot\left(\frac{\log y}{\log x}\right)^{\alpha^2+\beta^2}\left(\left(1+\min\left\{\frac{\log y}{\log x}, \frac{|t_1+t_2|^{-1}}{\log x}\right\}\right)\left(1+\min\left\{\frac{\log y}{\log x}, \frac{|t_1-t_2|^{-1}}{\log x}\right\}\right)\right)^{2\alpha\beta}.$$

As an upper bound, we may replace the error term $e^{O(\max\{\alpha,\beta,\alpha^2,\beta^2\}(1+(|t_1|+|t_2|)/(\log^{100} x)))}$ by

$$e^{O(\max\{\alpha,\beta,\alpha^2,\beta^2\})}\min\left\{\frac{\log y}{\log x}, 1+\frac{(|t_1|+|t_2|)^{1/100}}{\log x}\right\}^{|\alpha^2-\alpha|+|\beta^2-\beta|+4\alpha\beta},$$

and as a lower bound we may replace it by

$$e^{O(\max\{\alpha,\beta,\alpha^2,\beta^2\})} \min\left\{\frac{\log y}{\log x}, 1+\frac{(|t_1|+|t_2|)^{1/100}}{\log x}\right\}^{-(|\alpha^2-\alpha|+|\beta^2-\beta|+4\alpha\beta)}.$$

The estimation of the error terms here is rather crude, but will be sufficient as they only depend quite mildly on the t_i.

Proof of Euler Product Result 2.2. The proof is a fairly straightforward adaptation of the proof of Euler Product Result 2.1. We again temporarily set $M = M(\alpha,\beta) := \max\{\alpha,\beta,\alpha^3,\beta^3\}$. In the first place we have

$$\begin{aligned}
&\left|1+\frac{f(p)}{p^{1/2+\sigma+it_1}}\right|^{2\alpha}\left|1+\frac{f(p)}{p^{1/2+\sigma+it_2}}\right|^{2\beta} \\
&\quad= \exp\left\{2\alpha\Re\log\left(1+\frac{f(p)}{p^{1/2+\sigma+it_1}}\right)+2\beta\Re\log\left(1+\frac{f(p)}{p^{1/2+\sigma+it_2}}\right)\right\} \\
&\quad= \exp\left\{\frac{2\alpha\Re f(p)p^{-it_1}}{p^{1/2+\sigma}}-\frac{\alpha\Re f(p)^2p^{-2it_1}}{p^{1+2\sigma}}+\frac{2\beta\Re f(p)p^{-it_2}}{p^{1/2+\sigma}}-\frac{\beta\Re f(p)^2p^{-2it_2}}{p^{1+2\sigma}}+O\left(\frac{\max\{\alpha,\beta\}}{p^{3/2+3\sigma}}\right)\right\} \\
&\quad= 1+\frac{2(\alpha\Re f(p)p^{-it_1}+\beta\Re f(p)p^{-it_2})}{p^{1/2+\sigma}}-\frac{(\alpha\Re f(p)^2p^{-2it_1}+\beta\Re f(p)^2p^{-2it_2})}{p^{1+2\sigma}}+ \\
&\qquad\qquad+\frac{2(\alpha\Re f(p)p^{-it_1}+\beta\Re f(p)p^{-it_2})^2}{p^{1+2\sigma}}+O\left(\frac{M}{p^{3/2+3\sigma}}\right).
\end{aligned}$$

Furthermore, in the Rademacher case we have $f(p)^2 \equiv 1$, whilst still

$$\mathbb{E}\Re f(p)p^{-it} = \cos(t\log p)\mathbb{E}f(p) = 0.$$

So we get

$$\begin{aligned}
&\mathbb{E}\left|1+\frac{f(p)}{p^{1/2+\sigma+it_1}}\right|^{2\alpha}\left|1+\frac{f(p)}{p^{1/2+\sigma+it_2}}\right|^{2\beta} \\
&\quad= 1-\frac{(\alpha\cos(2t_1\log p)+\beta\cos(2t_2\log p))}{p^{1+2\sigma}}+\frac{2(\alpha\cos(t_1\log p)+\beta\cos(t_2\log p))^2}{p^{1+2\sigma}}+O\left(\frac{M}{p^{3/2+3\sigma}}\right),
\end{aligned}$$

and using standard cosine identities this is all

$$\begin{aligned}
&= 1+\frac{\alpha^2+\beta^2+(\alpha^2-\alpha)\cos(2t_1\log p)+(\beta^2-\beta)\cos(2t_2\log p)}{p^{1+2\sigma}}+ \\
&\qquad\qquad+\frac{2\alpha\beta(\cos((t_1+t_2)\log p)+\cos((t_1-t_2)\log p))}{p^{1+2\sigma}}+O\left(\frac{M}{p^{3/2+3\sigma}}\right) \\
&= \exp\left\{\frac{\alpha^2+\beta^2+(\alpha^2-\alpha)\cos(2t_1\log p)+(\beta^2-\beta)\cos(2t_2\log p)}{p^{1+2\sigma}}+\right. \\
&\qquad\qquad\left.+\frac{2\alpha\beta(\cos((t_1+t_2)\log p)+\cos((t_1-t_2)\log p))}{p^{1+2\sigma}}+O\left(\frac{M}{p^{3/2+3\sigma}}\right)\right\}.
\end{aligned}$$

The first two conclusions of Euler Product Result 2.2 now follow exactly as in the proof of Euler Product Result 2.1.

For the final claimed inequalities, we note that the source of the unwanted error term

$$O\left(\max\{\alpha, \beta, \alpha^2, \beta^2\}\frac{|t_1|+|t_2|}{\log^{100} x}\right)$$

in the exponent lies in our using the prime number theorem to estimate the various sums

$$\sum_{x<p\le y} \frac{(\alpha^2-\alpha)\cos(2t_1\log p)}{p^{1+2\sigma}},$$
$$\sum_{x<p\le y} \frac{(\beta^2-\beta)\cos(2t_2\log p)}{p^{1+2\sigma}},$$
$$\sum_{x<p\le y} \frac{2\alpha\beta\cos((t_1+t_2)\log p)}{p^{1+2\sigma}},$$
$$\sum_{x<p\le y} \frac{2\alpha\beta\cos((t_1-t_2)\log p)}{p^{1+2\sigma}}.$$

Instead, if $|t_1| \ge \log^{100} x$ (which is the only case where it might produce a large error term) we can upper bound $\sum_{x<p\le y}(\alpha^2-\alpha)\cos(2t_1\log p)/p^{1+2\sigma}$ by

$$\sum_{x<p\le \min\{e^{|t_1|^{1/100}},y\}} \frac{|\alpha^2-\alpha|}{p^{1+2\sigma}} + \sum_{\min\{e^{|t_1|^{1/100}},y\}<p\le y} \frac{(\alpha^2-\alpha)\cos(2t_1\log p)}{p^{1+2\sigma}}.$$

As in the proof of Euler Product Result 2.1, the second sum here is $\ll \max\{\alpha, \alpha^2\}$ (we can use the prime number theorem to estimate it, since the lower end point is now sufficiently large that we don't pick up a big error term), and the first sum is

$$|\alpha^2-\alpha|\left(\sum_{x<p\le \min\{e^{|t_1|^{1/100}},y\}} \frac{1}{p} + O(1)\right) = |\alpha^2-\alpha|\left(\min\left\{\log\left(\frac{\log y}{\log x}\right), \log\left(\frac{|t_1|^{1/100}}{\log x}\right)\right\} + O(1)\right).$$

We can handle the other sums similarly when t_2, t_1+t_2, t_1-t_2 are large. In the worst case, as an upper bound this will produce an extra multiplicative factor

$$\exp\left\{(|\alpha^2-\alpha|+|\beta^2-\beta|+4\alpha\beta)\min\left\{\log\left(\frac{\log y}{\log x}\right), \log\left(1+\frac{(|t_1|+|t_2|)^{1/100}}{\log x}\right)\right\}\right\}.$$

An exactly similar argument gives a lower bound with $(|\alpha^2-\alpha|+|\beta^2-\beta|+4\alpha\beta)$ replaced by $-(|\alpha^2-\alpha|+|\beta^2-\beta|+4\alpha\beta)$. □

Probabilistic preparations. Next we record some moment estimates, mostly fairly simple yet interesting, that will be input to our arguments in various places.

Probability Result 2.3 (Rough hypercontractive inequalities). *For any real $q \geq 1$, the following is true.*

If $f(n)$ is a Steinhaus random multiplicative function, then for any sequence of complex numbers $(a_n)_{n \leq N}$ we have

$$\mathbb{E}\Big|\sum_{n \leq N} a_n f(n)\Big|^{2q} \leq \Big(\sum_{n \leq N} |a_n|^2 d_{\lceil q \rceil}(n)\Big)^q,$$

where $d_k(\cdot)$ denotes the k-fold divisor function (i.e., the number of k-tuples of natural numbers whose product is $\cdot$, or equivalently the Dirichlet series coefficient of $\zeta(s)^k$), and $\lceil q \rceil$ denotes the ceiling of q.

If $f(n)$ is a Rademacher random multiplicative function, then for any sequence of complex numbers $(a_n)_{n \leq N}$ we have

$$\mathbb{E}\Big|\sum_{n \leq N} a_n f(n)\Big|^{2q} \leq \Big(\sum_{n \leq N} |a_n|^2 d_{2\lceil q \rceil - 1}(n)\Big)^q.$$

Proof of Probability Result 2.3. By Hölder's inequality, for any real $q \geq 1$ we have

$$\mathbb{E}\Big|\sum_{n \leq N} a_n f(n)\Big|^{2q} \leq \Big(\mathbb{E}\Big|\sum_{n \leq N} a_n f(n)\Big|^{2\lceil q \rceil}\Big)^{q/\lceil q \rceil},$$

so (replacing q by $\lceil q \rceil$) it suffices to treat the case where q is a natural number.

For Steinhaus $f(n)$, expanding the $2q$-th power and taking expectations we get

$$\mathbb{E}\Big|\sum_{n \leq N} a_n f(n)\Big|^{2q} = \sum_{n_1, \ldots, n_q \leq N} a_{n_1} \cdots a_{n_q} \sum_{m_1, \ldots, m_q \leq N} \overline{a_{m_1} \cdots a_{m_q}} \mathbf{1}_{\prod_{i=1}^q n_i = \prod_{i=1}^q m_i},$$

where $\mathbf{1}$ denotes the indicator function. Using the upper bound

$$|a_{n_1} \cdots a_{n_q} \overline{a_{m_1} \cdots a_{m_q}}| \leq \big(\tfrac{1}{2}\big)(|a_{n_1} \cdots a_{n_q}|^2 + |a_{m_1} \cdots a_{m_q}|^2),$$

together with the symmetry of the n_i and the m_i, we deduce that

$$\mathbb{E}\Big|\sum_{n \leq N} a_n f(n)\Big|^{2q} \leq \sum_{n_1, \ldots, n_q \leq N} |a_{n_1} \cdots a_{n_q}|^2 \sum_{m_1, \ldots, m_q \leq N} \mathbf{1}_{\prod_{i=1}^q n_i = \prod_{i=1}^q m_i} \leq \sum_{n_1, \ldots, n_q \leq N} |a_{n_1} \cdots a_{n_q}|^2 d_q\Big(\prod_{i=1}^q n_i\Big).$$

Finally, since the function $d_q(\cdot)$ is submultiplicative we find the above is

$$\leq \sum_{n_1, \ldots, n_q \leq N} |a_{n_1} \cdots a_{n_q}|^2 d_q(n_1) \cdots d_q(n_q) = \Big(\sum_{n \leq N} |a_n|^2 d_q(n)\Big)^q.$$

In the Rademacher case, one needs a bit more involved argument. We refer the reader to Lemma 2 of Halász [1983], where this result is proved by induction on the exponent $2q$. We may remark that, since Rademacher $f(n)$ is only supported on squarefree n, we may assume that a_n is only nonzero for squarefree n, and then $d_{2\lceil q \rceil - 1}(n) = (2\lceil q \rceil - 1)^{\Omega(n)}$ where $\Omega(n)$ is the number of prime factors of n. The ultimate source of the factors $d_{2\lceil q \rceil - 1}(n)$ is that, when one expands the expectation in the inductive proof, the only surviving terms are those where the product $n_1 \cdots n_{2q}$ is a perfect square, so all the prime factors of n_{2q} must be repeated somewhere amongst the other terms $n_1, \dots, n_{2q-1}$. $\square$

We describe the inequalities in Probability Result 2.3 as "rough hypercontractive inequalities" because (if we take $2q$-th roots of both sides) they upper bound an L^{2q}-norm by a weighted L^2 norm without any other terms, but the weights $d_{\lceil q\rceil}(n)$, $d_{2\lceil q\rceil-1}(n)$ will not generally be the sharpest possible unless q is an integer. One can prove more precise results for noninteger q using more subtle interpolation techniques, see Section 2 of Bondarenko, Brevig, Saksman, Seip and Zhao [Bondarenko et al. 2018] for the Steinhaus case, and Chapitre III of Bonami [1970] for the Rademacher case (expressed in rather different notation). However, for our applications the extra precision in these inequalities will not be needed.

Probability Result 2.4. *Let $(\epsilon_n)_{n\le N}$ be a sequence of independent random variables, each satisfying $\mathbb{E}\epsilon_n = 0$ and $\mathbb{E}|\epsilon_n|^2 = 1$, and let $(a_n)_{n\le N}$ be a sequence of complex numbers. Then for any real $q \ge 1$, we have*

$$\mathbb{E}\Big|\sum_{n\le N} a_n\epsilon_n\Big|^{2q} \ge \Big(\sum_{n\le N}|a_n|^2\Big)^q.$$

Proof of Probability Result 2.4. Since we assume that $q \ge 1$, simply applying Hölder's inequality we get

$$\Big(\sum_{n\le N}|a_n|^2\Big)^q = \Big(\mathbb{E}\Big|\sum_{n\le N} a_n\epsilon_n\Big|^2\Big)^q \le \mathbb{E}\Big|\sum_{n\le N} a_n\epsilon_n\Big|^{2q}. \qquad \square$$

If the ϵ_n are Rademacher or Steinhaus random variables,[3] then Khintchine's inequality (see e.g., Lemma 3.8.1 of Gut [2013]) in fact implies that $\mathbb{E}\big|\sum_{n\le N} a_n\epsilon_n\big|^{2q} \asymp_q \big(\sum_{n\le N}|a_n|^2\big)^q$ for all real $q \ge 0$. For our purposes here we will only require the simple lower bound in Probability Result 2.4, but it is useful to keep Khintchine's inequality in mind since it means that when we apply the lower bound, we are doing something sharp.

The final result we shall record is more sophisticated, and requires some terminology before we can state it. Suppose that $(\Omega, \mathcal{F}, \mathbb{P})$ is a probability space, and $(\mathcal{F}_n)_{n\ge0}$ is a *filtration* on $\mathcal{F}$, in other words a sequence of sub-σ-algebras satisfying $\mathcal{F}_0 \subseteq \mathcal{F}_1 \subseteq \cdots \subseteq \mathcal{F}$. We say a sequence of random variables $(X_n)_{n\ge0}$ on $(\Omega, \mathcal{F}, \mathbb{P})$ is a *submartingale* (relative to $(\mathcal{F}_n)_{n\ge0}$ and $\mathbb{P}$) if it satisfies:

(i) (adapted) X_n is measurable with respect to $\mathcal{F}_n$, for all $n \ge 0$.

(ii) (integrable) $\mathbb{E}|X_n|$ is finite, for all $n \ge 0$;

(iii) (nondecreasing on average) For all $n \ge 1$, the conditional expectation $\mathbb{E}(X_n \mid \mathcal{F}_{n-1}) \ge X_{n-1}$ almost surely.

Condition (iii) says that a submartingale is nondecreasing on average, in quite a strong sense: for any given value of X_{n-1} (or, informally speaking, any other "information" from the sigma algebra $\mathcal{F}_{n-1}$), the conditional expectation of X_n will be at least as large. One can apply this property to partition the sample

[3]We emphasize that here we are referring to ordinary Rademacher or Steinhaus random variables, not random *multiplicative* functions.

space Ω in useful ways, and prove that the moments of the random variables comprising a submartingale satisfy the following useful bound. We will use this as an ingredient in proving our $2q$-th moment upper bounds when q is close to 1.

Probability Result 2.5 (Doob's L^p maximal inequality, see Theorem 9.4 of Gut [2013]). *Let $(X_n)_{n\geq 0}$ be a nonnegative submartingale (on some probability space and with respect to some filtration). Then for any $p > 1$, we have*

$$\mathbb{E}(\max_{0\leq k\leq n} X_k)^p \leq \left(\frac{p}{p-1}\right)^p \mathbb{E}X_n^p.$$

Some miscellaneous lemmas. As in the first paper [Harper 2017] in this sequence, we will need the following version of Parseval's identity for Dirichlet series to help with relating $\mathbb{E}\left|\sum_{n\leq x} f(n)\right|^{2q}$ to an Euler product average.

Harmonic Analysis Result 2.6 (See (5.26) in Section 5.1 of [Montgomery and Vaughan 2007]). *Let $(a_n)_{n=1}^{\infty}$ be any sequence of complex numbers, and let $A(s) := \sum_{n=1}^{\infty} a_n/n^s$ denote the corresponding Dirichlet series, and σ_c denote its abscissa of convergence. Then for any $\sigma > \max\{0, \sigma_c\}$, we have*

$$\int_0^\infty \frac{\left|\sum_{n\leq x} a_n\right|^2}{x^{1+2\sigma}} dx = \frac{1}{2\pi}\int_{-\infty}^{\infty} \left|\frac{A(\sigma+it)}{\sigma+it}\right|^2 dt.$$

We will use the following estimate to handle sums of divisor-type functions that appear in our calculations.

Number Theory Result 2.7. *Let $0 < \delta < 1$, let $m \geq 1$, and suppose that $\max\{3, 2m\} \leq y \leq z \leq y^{10}$ and that $1 < u \leq v(1-y^{-\delta})$. As usual, let $\Omega(d)$ denote the total number of prime factors of d (counted with multiplicity). Then*

$$\sum_{\substack{u\leq d\leq v,\\ p\,|\,d \Rightarrow y\leq p\leq z}} m^{\Omega(d)} \ll_\delta \frac{(v-u)m}{\log y} \prod_{y\leq p\leq z}\left(1-\frac{m}{p}\right)^{-1}.$$

This is a slight generalization of a result of Lau, Tenenbaum and Wu [2013, Lemma 2.1] (see also [Halász 1983, Lemma 3]). See [Harper 2017, Section 2.1] for the full (short) proof.

3. Easier cases of the theorems

As remarked in the Introduction, since we allow a multiplicative error term $e^{O(q^2)}$ in our theorems, it turns out that proving our claimed upper bounds when $\log\log x \leq q \leq c\log x/\log\log x$ is somewhat straightforward. We present these arguments in this section. Some of the techniques involved, including the use of Rankin's trick with an exponent roughly like $1+q/\log x$, and a special treatment of prime factors that are $\ll q^2$, will recur later when we develop our main arguments.

The upper bound in the Steinhaus case, for very large q. For $q \geq \log\log x$ we have $\log^{(q-1)^2} x = \log^{q^2+O(q)} x = e^{O(q^2)} \log^{q^2} x$. Thus to establish the upper bound part of Theorem 1.1 for $\log\log x \leq q \leq c\log x/\log\log x$, it will suffice to show that

$$\Big\| \sum_{n\leq x} f(n) \Big\|_{2q} \leq e^{-(q/2)\log q-(q/2)\log\log(2q)+O(q)}\sqrt{x}\log^{q/2} x,$$

where as usual we write $\|\cdot\|_r := (\mathbb{E}|\cdot|^r)^{1/r}$.

To prove this, we first apply Minkowski's inequality to obtain that

$$\Big\| \sum_{n\leq x} f(n) \Big\|_{2q} = \Big\| \sum_{\substack{m\leq x, \\ m \text{ is } q^2 \text{ smooth}}} f(m) \sum_{\substack{n\leq x/m, \\ p|n\Rightarrow p>q^2}} f(n) \Big\|_{2q} \leq \sum_{\substack{m\leq x, \\ m \text{ is } q^2 \text{ smooth}}} \Big\| \sum_{\substack{n\leq x/m, \\ p|n\Rightarrow p>q^2}} f(n) \Big\|_{2q}.$$

Recall here that a number is said to be q^2-smooth if all of its prime factors are $\leq q^2$. Using the first part of Probability Result 2.3, and then using Rankin's trick of upper bounding $\mathbf{1}_{n\leq x/m}$ by $(x/(nm))^{1+q/\log x}$ (and recalling that the divisor function $d_{\lceil q\rceil}(n)$ is the Dirichlet series coefficient of $\zeta(s)^{\lceil q\rceil} = \sum_{n=1}^{\infty} d_{\lceil q\rceil}(n)/n^s = \prod_p (1-1/p^s)^{-\lceil q\rceil}$), we get

$$\begin{aligned}\Big\| \sum_{\substack{n\leq x/m, \\ p|n\Rightarrow p>q^2}} f(n) \Big\|_{2q} &\leq \Big(\sum_{\substack{n\leq x/m, \\ p|n\Rightarrow p>q^2}} d_{\lceil q\rceil}(n) \Big)^{1/2} \\ &\leq \Big(\Big(\frac{x}{m}\Big)^{1+q/\log x} \sum_{\substack{n\leq x/m, \\ p|n\Rightarrow p>q^2}} \frac{d_{\lceil q\rceil}(n)}{n^{1+q/\log x}} \Big)^{1/2} \\ &\leq \sqrt{\frac{x}{m}} e^{O(q)} \prod_{p>q^2} \Big(1-\frac{1}{p^{1+q/\log x}}\Big)^{-\lceil q\rceil/2}.\end{aligned}$$

Finally, the product over primes here is $\zeta(1+q/\log x)^{\lceil q\rceil/2}\prod_{p\leq q^2}(1-1/p^{1+q/\log x})^{\lceil q\rceil/2}$. Using the fact that the zeta function has a simple pole at 1, this equals $e^{O(q)}(\log x/q)^{\lceil q\rceil/2} e^{-\sum_{p\leq q^2}(\lceil q\rceil/2)/(p^{1+q/\log x})} = e^{O(q)}(\log x/q\log q)^{q/2}$ on our range $\log\log x \leq q \leq c\log x/\log\log x$. And when we sum over m we have $\sum_{m\leq x, m \text{ is } q^2 \text{ smooth}} 1/\sqrt{m} \leq e^{\sum_{p\leq q^2} O(1/\sqrt{p})} \leq e^{O(q)}$, so putting everything together we get an acceptable upper bound for $\|\sum_{n\leq x} f(n)\|_{2q}$.

□

The upper bound in the Rademacher case, for very large q. Similarly as in the Steinhaus case, to prove the upper bound part of Theorem 1.2 for $\log\log x \leq q \leq c\log x/\log\log x$ it will suffice to show that, for Rademacher random multiplicative $f(n)$, we have

$$\Big\| \sum_{n\leq x} f(n) \Big\|_{2q} \leq e^{-q\log q-q\log\log(2q)+O(q)}\sqrt{x}\log^{q} x.$$

Using Minkowski's inequality, the second part of Probability Result 2.3, and then Rankin's trick, we get

$$\Big\|\sum_{n\le x} f(n)\Big\|_{2q} \le \sum_{\substack{m\le x,\\ m \text{ is } q^2 \text{ smooth}}} \Big\| \sum_{\substack{n\le x/m,\\ p|n\Rightarrow p>q^2}} f(n)\Big\|_{2q}$$
$$\le \sum_{\substack{m\le x,\\ m \text{ is } q^2 \text{ smooth}}} \Big(\sum_{\substack{n\le x/m,\\ p|n\Rightarrow p>q^2}} d_{2\lceil q\rceil -1}(n)\Big)^{1/2}$$
$$\le \sum_{\substack{m\le x,\\ m \text{ is } q^2 \text{ smooth}}} \sqrt{\frac{x}{m}} e^{O(q)} \prod_{p>q^2}\Big(1-\frac{1}{p^{1+q/\log x}}\Big)^{-(2\lceil q\rceil -1)/2}.$$

We can estimate the product over primes as in the Steinhaus case, finding it is

$$e^{O(q)}\Big(\frac{\log x}{q}\Big)^{(2\lceil q\rceil -1)/2} e^{-\sum_{p\le q^2}((2\lceil q\rceil -1)/2)/p^{1+q/\log x}} = e^{O(q)}\Big(\frac{\log x}{q\log q}\Big)^{q}$$

on our range $\log\log x \le q \le c\log x/\log\log x$. And when we sum over m we again have

$$\sum_{\substack{m\le x,\\ m \text{ is } q^2 \text{ smooth}}} \frac{1}{\sqrt{m}} \le e^{\sum_{p\le q^2} O(1/\sqrt{p})} \le e^{O(q)},$$

so putting everything together we get an acceptable upper bound for $\|\sum_{n\le x} f(n)\|_{2q}$. □

4. The reduction to Euler products

In this section we shall prove four propositions that make precise the assertion in (1-2) that $\mathbb{E}|\sum_{n\le x} f(n)|^{2q}$ may be bounded by studying integrals of Euler products.

Upper bounds: statement of the propositions. We will need a little notation, which is exactly the same as in the author's previous paper [Harper 2017] dealing with low moments. Given a random multiplicative function $f(n)$ (either Steinhaus or Rademacher, depending on the context), and an integer $0\le k\le \log\log x$, let F_k denote the partial Euler product of $f(n)$ over $x^{e^{-(k+1)}}$-smooth numbers. Thus for all complex s with $\Re(s)>0$, we have

$$F_k(s) = \prod_{p\le x^{e^{-(k+1)}}} \Big(1-\frac{f(p)}{p^s}\Big)^{-1} = \sum_{\substack{n=1,\\ n \text{ is } x^{e^{-(k+1)}} \text{ smooth}}}^{\infty} \frac{f(n)}{n^s}$$

in the Steinhaus case, and

$$F_k(s) = \prod_{p\le x^{e^{-(k+1)}}} \Big(1+\frac{f(p)}{p^s}\Big) = \sum_{\substack{n=1,\\ n \text{ is } x^{e^{-(k+1)}} \text{ smooth}}}^{\infty} \frac{f(n)}{n^s}$$

in the Rademacher case (the product taking a different form because $f(n)$ is only supported on squarefree numbers in that case).

Proposition 4.1. *Let $f(n)$ be a Steinhaus random multiplicative function, let x be large, and set $\mathcal{L} := \lfloor (\log\log x)/10 \rfloor$. Uniformly for all $1 \le q \le \log^{0.05} x$, we have*

$$\Big\| \sum_{n \le x} f(n) \Big\|_{2q} \le \sqrt{\frac{x}{\log x}} e^{O(q)} \sum_{0 \le k \le \mathcal{L}} \bigg\| \int_{-1/2}^{1/2} \Big| F_k\Big(\frac{1}{2} + \frac{q-k}{\log x} + it\Big) \Big|^2 \, dt \bigg\|_q^{1/2} + e^{O(q)} \sqrt{\frac{x}{\log x}}.$$

In the low moments case, Proposition 1 of [Harper 2017] gives an analogous upper bound for all $\frac{2}{3} \le q \le 1$, but with the quantity $\mathcal{L}$ replaced by the smaller quantity $\mathcal{K} = \lfloor \log\log\log x \rfloor$, and the shift $(q-k)/\log x$ in the Euler product replaced by $-k/\log x$.

The additional shift by $q/\log x$ here corresponds to applying Rankin's trick with exponent $1 + q/\log x$ in our treatment of very large q in Section 3. We can introduce this at the acceptable cost of a prefactor $e^{O(q)}$ in the proposition, and it means that when we analyze the Euler product we can restrict attention to numbers that are $x^{1/q}$-smooth, which is crucial to obtaining the desired factor $e^{-q^2 \log q}$ in Theorem 1.1. The significant contribution from very smooth numbers, when q becomes large, also explains why we must let k run over a wider range than in the low moments case to obtain acceptable bounds. Finally, we remark that the range $1 \le q \le \log^{0.05} x$ allowed in Proposition 4.1 is somewhat artificial, but more than sufficient since we already proved the Theorem 1.1 upper bound for all $\log\log x \le q \le c \log x/\log\log x$ in Section 3. It could be increased somewhat, but it seems hard to obtain an upper bound of a similar shape to Proposition 4.1 on the full range $1 \le q \le c \log x/\log\log x$, since for very large q the significant contribution from very smooth numbers changes the behavior in parts of the proof.

Proposition 4.2. *Let $f(n)$ be a Rademacher random multiplicative function, let x be large, and set $\mathcal{L} := \lfloor (\log\log x)/10 \rfloor$. Uniformly for all $1 \le q \le \log^{0.05} x$, we have*

$$\Big\| \sum_{n \le x} f(n) \Big\|_{2q} \le \sqrt{\frac{x}{\log x}} e^{O(q)} \sum_{0 \le k \le \mathcal{L}} \max_{N \in \mathbb{Z}} \frac{1}{(|N|+1)^{1/8}} \bigg\| \int_{N-1/2}^{N+1/2} \Big| F_k\Big(\frac{1}{2} + \frac{q-k}{\log x} + it\Big) \Big|^2 \, dt \bigg\|_q^{1/2} + e^{O(q)} \sqrt{\frac{x}{\log x}}.$$

One has to deal with translates by N in the Rademacher case because, unlike in the Steinhaus case, the distribution of $(f(n)n^{it})$ is *not* the same (for $t \neq 0$) as the distribution of $(f(n))$ for Rademacher random multiplicative $f(n)$. However, as in the low moments argument in [Harper 2017], the main contribution will come from small N.

Lower bounds: statement of the propositions. For our work on lower bounds, we again connect the size of $\| \sum_{n \le x} f(n) \|_{2q}$ with a certain integral average, and thence with random Euler products. Let F denote the partial Euler product of $f(n)$, either Steinhaus or Rademacher, over x-smooth numbers. (Thus $F = F_{-1}$, if we slightly abuse our earlier notation).

Proposition 4.3. *If $f(n)$ is a Steinhaus random multiplicative function, and x is large, then uniformly for all $q \geq 1$ we have*

$$\Big\| \sum_{n \leq x} f(n) \Big\|_{2q} \gg \sqrt{\frac{x}{\log x}} \Big\| \int_1^{x^{1/4}} \Big| \sum_{m \leq z} f(m) \Big|^2 \frac{dz}{z^2} \Big\|_q^{1/2}.$$

In particular, for any large quantity $V \leq (\log x)/q$ we have that $\| \sum_{n \leq x} f(n) \|_{2q}$ is

$$\gg \sqrt{\frac{x}{\log x}} \bigg(\Big\| \int_{-1/2}^{1/2} \Big| F\Big(\frac{1}{2} + \frac{4Vq}{\log x} + it\Big) \Big|^2 dt \Big\|_q^{1/2} - \frac{C}{e^{Vq/2}} \Big\| \int_{-1/2}^{1/2} \Big| F\Big(\frac{1}{2} + \frac{2Vq}{\log x} + it\Big) \Big|^2 dt \Big\|_q^{1/2} \bigg),$$

where $C > 0$ is an absolute constant.

Notice that we don't need to impose any upper bound on q here (although, for the second statement, there is an implicit upper bound $q \ll \log x$ in order that we can choose large $V \leq (\log x)/q$). This means we can use Proposition 4.3 to prove the lower bound in Theorem 1.1 on the full range of q there.

Proposition 4.4. *If $f(n)$ is a Rademacher random multiplicative function, then the first bound in Proposition 4.3 continues to hold, and the second bound may be replaced by the statement that*

$$\Big\| \sum_{n \leq x} f(n) \Big\|_{2q} \gg \sqrt{\frac{x}{\log x}} \bigg(\Big\| \int_{-1/2}^{1/2} \Big| F\Big(\frac{1}{2} + \frac{4Vq}{\log x} + it\Big) \Big|^2 dt \Big\|_q^{1/2} - \frac{C}{e^{Vq/2}} \max_{N \in \mathbb{Z}} \frac{1}{(|N|+1)^{1/8}} \Big\| \int_{N-1/2}^{N+1/2} \Big| F\Big(\frac{1}{2} + \frac{2Vq}{\log x} + it\Big) \Big|^2 dt \Big\|_q^{1/2} \bigg).$$

These results are again of the same general shape as the corresponding Propositions 3 and 4 of [Harper 2017] from the low moments case. In fact, the propositions here are a little simpler as they don't involve an additional subtracted error term $-C\sqrt{x/\log x}$. This is accomplished by some reorganization of the proof, and shrinking the range of integration over z to $[1, x^{1/4}]$ rather than $[1, \sqrt{x}]$ from the low moments case, which makes no difference when applying the results. The other difference, similarly as in Section 3 and in our discussion of upper bounds, is that here we introduce shifts of the shape $4Vq/\log x$ in our Euler products, as opposed to $4V/\log x$ in the low moments analogues.

Proof of Propositions 4.1 and 4.2. We begin with Proposition 4.1. Let $P(n)$ denote the largest prime factor of n, and recall that a number n is said to be y-smooth if $P(n) \leq y$. Recall also that the divisor function $d_{\lceil q \rceil}(n)$ is the Dirichlet series coefficient of $\zeta(s)^{\lceil q \rceil} = \prod_p (1 - 1/p^s)^{-\lceil q \rceil}$. By Minkowski's inequality, we have

$$\Big\| \sum_{n \leq x} f(n) \Big\|_{2q} \leq \sum_{0 \leq k \leq \mathcal{L}} \Big\| \sum_{\substack{n \leq x, \\ x^{e^{-(k+1)}} < P(n) \leq x^{e^{-k}}}} f(n) \Big\|_{2q} + \Big\| \sum_{\substack{n \leq x, \\ P(n) \leq x^{e^{-(\mathcal{L}+1)}}}} f(n) \Big\|_{2q}.$$

Furthermore, the first part of Probability Result 2.3, followed by Rankin's trick with exponent $1-1/\log^{0.9} x$ (bounding $\mathbf{1}_{n\le x}$ by $\left(\frac{x}{n}\right)^{1-1/\log^{0.9} x} = xe^{-\log^{0.1} x}\frac{1}{n^{1-1/\log^{0.9} x}}$), implies that

$$\Bigg\| \sum_{\substack{n\le x,\\ P(n)\le x^{e^{-(\mathcal{L}+1)}}}} f(n)\Bigg\|_{2q} \le \Bigg[\sum_{\substack{n\le x,\\ P(n)\le x^{e^{-(\mathcal{L}+1)}}}} d_{\lceil q\rceil}(n)\Bigg]^{1/2} \le \Bigg[xe^{-\log^{0.1} x}\sum_{\substack{n\le x,\\ P(n)\le x^{e^{-(\mathcal{L}+1)}}}} \frac{d_{\lceil q\rceil}(n)}{n^{1-1/\log^{0.9} x}}\Bigg]^{1/2}.$$

Here the sum over n is $\le \prod_{p\le x^{e^{-(\mathcal{L}+1)}}}(1-1/p^{1-1/\log^{0.9} x})^{-\lceil q\rceil}$, and recalling that $\mathcal{L} := \lfloor(\log\log x)/10\rfloor$ this is $\le \prod_{p\le e^{\log^{0.9} x}}(1-1/p^{1-1/\log^{0.9} x})^{-\lceil q\rceil}$, which is $= e^{O(q)}\prod_{p\le e^{\log^{0.9} x}}(1-1/p)^{-\lceil q\rceil} = \log^{O(q)} x$ by standard Chebychev and Mertens estimates for sums over primes. Since we assume in Proposition 4.1 that $q\le \log^{0.05} x$, this whole contribution is $\ll \sqrt{x}e^{-c\log^{0.1} x}$, which is more than acceptable.

Next, if we let $\mathbb{E}^{(k)}$ denote expectation conditional on $(f(p))_{p\le x^{e^{-(k+1)}}}$, then the first part of Probability Result 2.3 applied, after conditioning on $(f(p))_{p\le x^{e^{-(k+1)}}}$, with

$$a_m = \mathbf{1}_{p\,|\,m\Rightarrow x^{e^{-(k+1)}}<p\le x^{e^{-k}}}\cdot \sum_{\substack{n\le x/m,\\ n \text{ is } x^{e^{-(k+1)}}\text{-smooth}}} f(n)$$

implies

$$\begin{aligned}
\sum_{0\le k\le\mathcal{L}}\Bigg\| \sum_{\substack{n\le x,\\ x^{e^{-(k+1)}}<P(n)\le x^{e^{-k}}}} f(n)\Bigg\|_{2q} &= \sum_{0\le k\le\mathcal{L}}\Bigg\| \sum_{\substack{1<m\le x,\\ p\,|\,m\Rightarrow x^{e^{-(k+1)}}<p\le x^{e^{-k}}}} f(m)\sum_{\substack{n\le x/m,\\ n \text{ is } x^{e^{-(k+1)}}\text{-smooth}}} f(n)\Bigg\|_{2q}\\
&= \sum_{0\le k\le\mathcal{L}}\Bigg(\mathbb{E}\mathbb{E}^{(k)}\Bigg| \sum_{\substack{1<m\le x,\\ p\,|\,m\Rightarrow x^{e^{-(k+1)}}<p\le x^{e^{-k}}}} f(m)\sum_{\substack{n\le x/m,\\ n \text{ is } x^{e^{-(k+1)}}\text{-smooth}}} f(n)\Bigg|^{2q}\Bigg)^{1/2q}\\
&\le \sum_{0\le k\le\mathcal{L}}\Bigg(\mathbb{E}\Bigg(\sum_{\substack{1<m\le x,\\ p\,|\,m\Rightarrow x^{e^{-(k+1)}}<p\le x^{e^{-k}}}} d_{\lceil q\rceil}(m)\Bigg|\sum_{\substack{n\le x/m,\\ n \text{ is } x^{e^{-(k+1)}}\text{-smooth}}} f(n)\Bigg|^2\Bigg)^q\Bigg)^{1/2q}.
\end{aligned}$$

To proceed further, we want to replace $\left|\sum_{n\le x/m,\ n \text{ is } x^{e^{-(k+1)}}\text{-smooth}} f(n)\right|^2$ in the above by a smoothed version. Set $X = e^{\sqrt{\log x}}$, say, and note that (uniformly for any $1\le q\le \log^{0.05} x$) the above is

$$\begin{aligned}
&\sum_{0\le k\le\mathcal{L}}\Bigg\| \sum_{\substack{1<m\le x,\\ p\,|\,m\Rightarrow x^{e^{-(k+1)}}<p\le x^{e^{-k}}}} d_{\lceil q\rceil}(m)\Bigg|\sum_{\substack{n\le x/m,\\ n \text{ is } x^{e^{-(k+1)}}\text{-smooth}}} f(n)\Bigg|^2\Bigg\|_q^{1/2}\\
&\ll \sum_{0\le k\le\mathcal{L}}\Bigg\| \sum_{\substack{1<m\le x,\\ p\,|\,m\Rightarrow x^{e^{-(k+1)}}<p\le x^{e^{-k}}}} d_{\lceil q\rceil}(m)\frac{X}{m}\int_m^{m(1+1/X)}\Bigg|\sum_{\substack{n\le x/t,\\ x^{e^{-(k+1)}}\text{-smooth}}} f(n)\Bigg|^2 dt\Bigg\|_q^{1/2}\\
&\quad + \sum_{0\le k\le\mathcal{L}}\Bigg\| \sum_{\substack{1<m\le x,\\ p\,|\,m\Rightarrow x^{e^{-(k+1)}}<p\le x^{e^{-k}}}} d_{\lceil q\rceil}(m)\frac{X}{m}\int_m^{m(1+1/X)}\Bigg|\sum_{\substack{x/t<n\le x/m,\\ x^{e^{-(k+1)}}\text{-smooth}}} f(n)\Bigg|^2 dt\Bigg\|_q^{1/2}.
\end{aligned} \tag{4-1}$$

We next want to show that the second term in (4-1) may be discarded as an error term. Using Minkowski's inequality again, followed by Hölder's inequality with exponent q applied to the normalized integral $\frac{X}{m}\int_m^{m(1+1/X)} dt$, this second term is

$$\leq \sum_{0 \leq k \leq \mathcal{L}} \Bigg[\sum_{\substack{1<m \leq x, \\ p \mid m \Rightarrow x^{e^{-(k+1)}} < p \leq x^{e^{-k}}}} d_{\lceil q \rceil}(m) \Bigg\| \frac{X}{m} \int_m^{m(1+1/X)} \Bigg| \sum_{\substack{x/t < n \leq x/m, \\ x^{e^{-(k+1)}}\text{-smooth}}} f(n) \Bigg|^2 dt \Bigg\|_q \Bigg]^{1/2}$$

$$\leq \sum_{0 \leq k \leq \mathcal{L}} \Bigg[\sum_{\substack{1<m \leq x, \\ p \mid m \Rightarrow x^{e^{-(k+1)}} < p \leq x^{e^{-k}}}} d_{\lceil q \rceil}(m) \Bigg(\frac{X}{m} \int_m^{m(1+1/X)} \mathbb{E} \Bigg| \sum_{\substack{x/t < n \leq x/m, \\ x^{e^{-(k+1)}}\text{-smooth}}} f(n) \Bigg|^{2q} dt \Bigg)^{1/q} \Bigg]^{1/2}.$$

The length of the sum over n here is $x(t-m)/(mt) \leq x/(mX)$, so when $x/X \leq m \leq x$ there will be at most one term in the sum, and we simply have

$$\mathbb{E} \Bigg| \sum_{\substack{x/t < n \leq x/m, \\ x^{e^{-(k+1)}}\text{-smooth}}} f(n) \Bigg|^{2q} \leq 1.$$

When $x^{e^{-(k+1)}} < m < x/X$, we take a fairly crude approach and use the Cauchy–Schwarz inequality, obtaining that

$$\begin{aligned}
\mathbb{E} \Bigg| \sum_{\substack{x/t < n \leq x/m, \\ x^{e^{-(k+1)}}\text{-smooth}}} f(n) \Bigg|^{2q} &\leq \Bigg[\mathbb{E} \Bigg| \sum_{\substack{x/t < n \leq x/m, \\ x^{e^{-(k+1)}}\text{-smooth}}} f(n) \Bigg|^2 \mathbb{E} \Bigg| \sum_{\substack{x/t < n \leq x/m, \\ x^{e^{-(k+1)}}\text{-smooth}}} f(n) \Bigg|^{2(2q-1)} \Bigg]^{1/2} \\
&\ll \Bigg[\frac{x}{mX} \mathbb{E} \Bigg| \sum_{\substack{x/t < n \leq x/m, \\ x^{e^{-(k+1)}}\text{-smooth}}} f(n) \Bigg|^{2(2q-1)} \Bigg]^{1/2} \\
&\ll \Bigg[\frac{x}{mX} \Big(\frac{x}{m} \Big)^{2q-1} \log^{O(q^2)} x \Bigg]^{1/2} \\
&= \Big(\frac{x}{m} \Big)^q \frac{\log^{O(q^2)} x}{X^{1/2}}.
\end{aligned}$$

Here the crude upper bound $(x/m)^{2q-1} \log^{O(q^2)} x$ for the $2(2q-1)$-th moment may be proved as in Section 3.

Putting things together, we find that the second term in (4-1) is

$$\ll \sum_{0 \leq k \leq \mathcal{L}} \Bigg[\frac{x \log^{O(q)} x}{X^{1/2q}} \sum_{\substack{1<m<x/X, \\ p \mid m \Rightarrow x^{e^{-(k+1)}} < p \leq x^{e^{-k}}}} \frac{d_{\lceil q \rceil}(m)}{m} + \sum_{\substack{x/X \leq m \leq x, \\ p \mid m \Rightarrow x^{e^{-(k+1)}} < p \leq x^{e^{-k}}}} d_{\lceil q \rceil}(m) \Bigg]^{1/2}.$$

To bound the first of these sums we use the simple estimate

$$\sum_{\substack{1<m<x/X, \\ p\,|\,m \Rightarrow x^{e^{-(k+1)}}<p\le x^{e^{-k}}}} \frac{d_{\lceil q\rceil}(m)}{m} \le \prod_{x^{e^{-(k+1)}}<p\le x^{e^{-k}}} \left(1-\tfrac{1}{p}\right)^{-\lceil q\rceil},$$

which is $= e^{O(q)}$ by the Mertens estimate for products over primes. To bound the second sum, by submultiplicativity of $d_{\lceil q\rceil}(\cdot)$ we always have $d_{\lceil q\rceil}(m) \le \lceil q\rceil^{\Omega(m)}$, where $\Omega(m)$ is the total number of prime factors of m. And we note (to obtain good dependence on k) that if $m \ge x/X$ only has prime factors from the interval $(x^{e^{-(k+1)}}, x^{e^{-k}}]$, then we must have $\Omega(m) \ge e^k/2$, say. So we get that

$$\sum_{\substack{x/X\le m\le x, \\ p\,|\,m \Rightarrow x^{e^{-(k+1)}}<p\le x^{e^{-k}}}} d_{\lceil q\rceil}(m)$$

is at most

$$5^{-e^k/2} \sum_{\substack{x/X\le m\le x, \\ p\,|\,m \Rightarrow x^{e^{-(k+1)}}<p\le x^{e^{-k}}}} (5\lceil q\rceil)^{\Omega(m)} \ll 5^{-e^k/2}\frac{e^k q x}{\log x} \prod_{x^{e^{-(k+1)}}<p\le x^{e^{-k}}} \left(1-\frac{5\lceil q\rceil}{p}\right)^{-1} \ll \frac{e^{O(q)}2^{-e^k}x}{\log x},$$

where the first inequality uses Number Theory Result 2.7. Recalling that we have

$$q \le \log^{0.05} x, \quad \mathcal{L} = \lfloor (\log\log x)/10 \rfloor \quad \text{and} \quad X = e^{\sqrt{\log x}},$$

the second term in (4-1) is

$$\le \sum_{0\le k\le \mathcal{L}} \left[\frac{x\log^{O(q)} x}{X^{1/2q}} + e^{O(q)}2^{-e^k}\frac{x}{\log x}\right]^{1/2} \le e^{O(q)}\sqrt{\frac{x}{\log x}},$$

which is an acceptable contribution for Proposition 4.1.

Turning to the remaining first sum in (4-1), this is equal to

$$\sum_{0\le k\le \mathcal{L}} \left\| \int_{x^{e^{-(k+1)}}}^{x} \Bigg| \sum_{\substack{n\le x/t, \\ x^{e^{-(k+1)}}\text{-smooth}}} f(n) \Bigg|^2 \sum_{\substack{t/(1+1/X)\le m\le t, \\ p\,|\,m \Rightarrow x^{e^{-(k+1)}}<p\le x^{e^{-k}}}} \frac{X}{m} d_{\lceil q\rceil}(m)\, dt \right\|_q^{1/2}.$$

Now we set $u = u(k,t) := e^k(\log t)/\log x$, and notice that (by submultiplicativity) $d_{\lceil q\rceil}(m) \le \lceil q\rceil^{\Omega(m)}$, and if $m \ge t/(1+1/X)$ only has prime factors from the interval $(x^{e^{-(k+1)}}, x^{e^{-k}}]$ then we must have $\Omega(m) \ge u-1$. So using Number Theory Result 2.7 (whose conditions are satisfied since $X = e^{\sqrt{\log x}}$ isn't too large, and $k \le (\log\log x)/10$) we get

$$\sum_{\substack{t/(1+1/X)\le m\le t,\\ p\,|\,m\Rightarrow x^{e^{-(k+1)}}<p\le x^{e^{-k}}}} \frac{X}{m} d_{\lceil q\rceil}(m) \ll \frac{X}{t}5^{-u} \sum_{\substack{t/(1+1/X)\le m\le t,\\ p\,|\,m\Rightarrow x^{e^{-(k+1)}}<p\le x^{e^{-k}}}} (5\lceil q\rceil)^{\Omega(m)}$$
$$\ll \frac{qe^k 5^{-u}}{\log x} \prod_{x^{e^{-(k+1)}}<p\le x^{e^{-k}}} \left(1-\frac{5\lceil q\rceil}{p}\right)^{-1}$$
$$\ll \frac{e^{O(q)}}{\log t},$$

provided x is sufficiently large. Consequently, the first sum in (4-1) is

$$\le e^{O(q)} \sum_{0\le k\le \mathcal{L}} \left\| \int_{x^{e^{-(k+1)}}}^{x} \Bigl| \sum_{\substack{n\le x/t,\\ x^{e^{-(k+1)}}\text{-smooth}}} f(n)\Bigr|^2 \frac{dt}{\log t} \right\|_q^{1/2}$$
$$= e^{O(q)} \sum_{0\le k\le \mathcal{L}} \sqrt{x} \left\| \int_{1}^{x^{1-e^{-(k+1)}}} \Bigl| \sum_{\substack{n\le z,\\ x^{e^{-(k+1)}}\text{-smooth}}} f(n)\Bigr|^2 \frac{dz}{z^2\log(x/z)} \right\|_q^{1/2},$$

where the second line follows from making the substitution $z = x/t$.

To obtain a satisfactory dependence on k in our final estimations, we now note that if $z\le\sqrt{x}$ we have $\log(x/z)\gg\log x$, whereas if $\sqrt{x}<z\le x^{1-e^{-(k+1)}}$ we have $\log(x/z)\gg e^{-k}\log x$. Thus in any case we have $\log(x/z)\gg z^{-2k/\log x}\log x$. As discussed earlier, we also want to introduce a Rankin style shift, which we will achieve by adding a factor $(x/z)^{2q/\log x} = e^{O(q)}z^{-2q/\log x}$ into the integral. Inserting these estimates, we find the first sum in (4-1) is

$$\le \frac{\sqrt{x}e^{O(q)}}{\sqrt{\log x}} \sum_{0\le k\le \mathcal{L}} \left\| \int_{1}^{x^{1-e^{-(k+1)}}} \Bigl| \sum_{\substack{n\le z,\\ x^{e^{-(k+1)}}\text{-smooth}}} f(n)\Bigr|^2 \frac{dz}{z^{2+2q/\log x-2k/\log x}} \right\|_q^{1/2}.$$

Finally, using Harmonic Analysis Result 2.6 and then Minkowski's inequality, all of the above is

$$\le \sqrt{\frac{x}{\log x}}e^{O(q)} \sum_{0\le k\le \mathcal{L}} \left\| \int_{-\infty}^{\infty} \frac{|F_k(1/2+q/\log x-k/\log x+it)|^2}{|1/2+q/\log x-k/\log x+it|^2}\,dt \right\|_q^{1/2}$$
$$\le \sqrt{\frac{x}{\log x}}e^{O(q)} \sum_{0\le k\le \mathcal{L}} \left[\sum_{n\in\mathbb{Z}} \frac{1}{n^2+1} \left\| \int_{n-1/2}^{n+1/2} \left| F_k\left(\frac{1}{2}+\frac{q-k}{\log x}+it\right)\right|^2 dt \right\|_q \right]^{1/2},$$

where F_k denotes the partial Euler product of $f(n)$ over $x^{e^{-(k+1)}}$-smooth numbers. In the Steinhaus case, since the law of the random function $f(n)$ is the same as the law of $f(n)n^{it}$ for any fixed $t\in\mathbb{R}$ we have

$$\left\| \int_{n-1/2}^{n+1/2} \left| F_k\left(\frac{1}{2}+\frac{q-k}{\log x}+it\right)\right|^2 dt \right\|_q = \left\| \int_{-1/2}^{1/2} \left| F_k\left(\frac{1}{2}+\frac{q-k}{\log x}+it\right)\right|^2 dt \right\|_q \quad \forall n.$$

Proposition 4.1 now follows on putting everything together. □

The proof of Proposition 4.2, covering the Rademacher case, is very similar to the Steinhaus case. We use the Rademacher part of Probability Result 2.3, producing various terms $d_{2\lceil q\rceil-1}(n)$ in place of $d_{\lceil q\rceil}(n)$, but this doesn't alter the analysis. The only nontrivial change comes at the very end of the proof, where (since it is no longer the case that the law of the random function $f(n)$ is the same as the law of $f(n)n^{it}$) we apply the bound

$$\left[\sum_{n\in\mathbb{Z}}\frac{1}{n^2+1}\left\|\int_{n-1/2}^{n+1/2}\left|F_k\left(\frac{1}{2}+\frac{q-k}{\log x}+it\right)\right|^2 dt\right\|_q\right]^{1/2} \ll \left[\max_{N\in\mathbb{Z}}\frac{1}{(|N|+1)^{1/4}}\left\|\int_{N-1/2}^{N+1/2}\left|F_k\left(\frac{1}{2}+\frac{q-k}{\log x}+it\right)\right|^2 dt\right\|_q\right]^{1/2}. \qquad \square$$

Proof of Propositions 4.3 and 4.4. We proceed somewhat similarly to Section 2.5 of [Harper 2017] or Section 2.2 of [Harper et al. 2015].

Again we let $P(n)$ denote the largest prime factor of n, and we introduce an auxiliary Rademacher random variable ϵ that is independent of everything else. Then we find that

$$\begin{aligned}\Bigg\|\sum_{\substack{n\le x,\\ P(n)>x^{3/4}}} f(n)\Bigg\|_{2q} &= \tfrac{1}{2}\Bigg\|\sum_{\substack{n\le x,\\ P(n)>x^{3/4}}} f(n)+\sum_{\substack{n\le x,\\ P(n)\le x^{3/4}}} f(n)+\sum_{\substack{n\le x,\\ P(n)>x^{3/4}}} f(n)-\sum_{\substack{n\le x,\\ P(n)\le x^{3/4}}} f(n)\Bigg\|_{2q}\\ &\le \tfrac{1}{2}\Bigg(\Bigg\|\sum_{\substack{n\le x,\\ P(n)>x^{3/4}}} f(n)+\sum_{\substack{n\le x,\\ P(n)\le x^{3/4}}} f(n)\Bigg\|_{2q}+\Bigg\|\sum_{\substack{n\le x,\\ P(n)>x^{3/4}}} f(n)-\sum_{\substack{n\le x,\\ P(n)\le x^{3/4}}} f(n)\Bigg\|_{2q}\Bigg)\\ &\le \Bigg\|\epsilon\sum_{\substack{n\le x,\\ P(n)>x^{3/4}}} f(n)+\sum_{\substack{n\le x,\\ P(n)\le x^{3/4}}} f(n)\Bigg\|_{2q}\\ &= \Bigg\|\sum_{n\le x} f(n)\Bigg\|_{2q}.\end{aligned}$$

Here the first inequality is Minkowski's inequality; the second is Hölder's inequality (with exponent $2q$) applied only to the averaging over ϵ; and the final equality follows since the law of

$$\epsilon\sum_{\substack{n\le x,\\ P(n)>x^{3/4}}} f(n) = \epsilon\sum_{x^{3/4}<p\le x} f(p)\sum_{m\le x/p} f(m)$$

conditional on the values $(f(p))_{p\le x^{3/4}}$ is the same as the law of $\sum_{n\le x,\ P(n)>x^{3/4}} f(n)$.

Now in the decomposition

$$\sum_{n\le x,\ P(n)>x^{3/4}} f(n) = \sum_{x^{3/4}<p\le x} f(p)\sum_{m\le x/p} f(m),$$

the inner sums are determined by the values $(f(p))_{p\le x^{3/4}}$ (and in fact by the values $(f(p))_{p\le x^{1/4}}$), which are independent of the outer random variables $(f(p))_{x^{3/4}<p\le x}$. So conditioning on the values $(f(p))_{p\le x^{3/4}}$

determining the inner sums and applying Probability Result 2.4 with $a_p = \sum_{m \le x/p} f(m)$, it follows that

$$\Big\| \sum_{\substack{n \le x, \\ P(n) > x^{3/4}}} f(n) \Big\|_{2q} \ge \Big\| \sum_{x^{3/4} < p \le x} \Big| \sum_{m \le x/p} f(m) \Big|^2 \Big\|_q^{1/2} \ge \frac{1}{\sqrt{\log x}} \Big\| \sum_{x^{3/4} < p \le x} \log p \Big| \sum_{m \le x/p} f(m) \Big|^2 \Big\|_q^{1/2}.$$

Next we want to replace the sum over p by an integral average. We can rewrite

$$\sum_{x^{3/4} < p \le x} \log p \Big| \sum_{m \le x/p} f(m) \Big|^2 = \sum_{r \le x^{1/4}} \sum_{x/(r+1) < p \le x/r} \log p \Big| \sum_{m \le r} f(m) \Big|^2,$$

and noting that $x/r - x/(r+1) = x/(r(r+1)) \gg (x/r)^{2/3}$ on our range of r, a Hoheisel-type prime number theorem in short intervals (see, e.g., Theorem 12.8 of [Ivić 2003]) implies that

$$\sum_{x^{3/4} < p \le x} \log p \Big| \sum_{m \le x/p} f(m) \Big|^2 \gg \sum_{r \le x^{1/4}} \Big(\int_{x/(r+1)}^{x/r} 1 \, dt \Big) \Big| \sum_{m \le r} f(m) \Big|^2 \ge \int_{x^{3/4}}^{x} \Big| \sum_{m \le x/t} f(m) \Big|^2 dt.$$

Making a substitution $z = x/t$, we see this integral is the same as $x \int_1^{x^{1/4}} \big| \sum_{m \le z} f(m) \big|^2 \frac{dz}{z^2}$. Checking back, this completes the proof of the first part of Proposition 4.3.

To deduce the second part of Proposition 4.3, we note that for any large V and any $q \ge 1$ we have

$$\begin{aligned} \Big\| \int_1^{x^{1/4}} \Big| \sum_{m \le z} f(m) \Big|^2 \frac{dz}{z^2} \Big\|_q & \\ &\ge \Big\| \int_1^{x^{1/4}} \Big| \sum_{\substack{m \le z, \\ x\text{-smooth}}} f(m) \Big|^2 \frac{dz}{z^{2+8Vq/\log x}} \Big\|_q \\ &\ge \Big\| \int_1^{\infty} \Big| \sum_{\substack{m \le z, \\ x\text{-smooth}}} f(m) \Big|^2 \frac{dz}{z^{2+8Vq/\log x}} \Big\|_q - \Big\| \int_{x^{1/4}}^{\infty} \Big| \sum_{\substack{m \le z, \\ x\text{-smooth}}} f(m) \Big|^2 \frac{dz}{z^{2+8Vq/\log x}} \Big\|_q \\ &\ge \Big\| \int_1^{\infty} \Big| \sum_{\substack{m \le z, \\ x\text{-smooth}}} f(m) \Big|^2 \frac{dz}{z^{2+8Vq/\log x}} \Big\|_q - \frac{1}{e^{Vq}} \Big\| \int_1^{\infty} \Big| \sum_{\substack{m \le z, \\ x\text{-smooth}}} f(m) \Big|^2 \frac{dz}{z^{2+4Vq/\log x}} \Big\|_q. \end{aligned}$$

By Harmonic Analysis Result 2.6, provided that $V \le (\log x)/q$ (so that $Vq/\log x$ is uniformly bounded) the first term here is $\gg \big\| \int_{-1/2}^{1/2} \big| F\big(\frac{1}{2} + \frac{4Vq}{\log x} + it\big) \big|^2 dt \big\|_q$ and the subtracted second term is $\ll e^{-Vq} \big\| \int_{-\infty}^{\infty} \big| F\big(\frac{1}{2} + \frac{2Vq}{\log x} + it\big) \big|^2 / \big| \frac{1}{2} + \frac{2Vq}{\log x} + it \big|^2 dt \big\|_q$, which in the Steinhaus case is $\ll e^{-Vq} \big\| \int_{-1/2}^{1/2} \big| F\big(\frac{1}{2} + \frac{2Vq}{\log x} + it\big) \big|^2 dt \big\|_q$ by "translation invariance in law". Putting everything together, this finishes the proof of Proposition 4.3. □

The arguments in the Rademacher case are exactly the same until the final line, where we don't have "translation invariance" so we must upper bound $\big\| \int_{-\infty}^{\infty} \big| F\big(\frac{1}{2} + \frac{2Vq}{\log x} + it\big) \big|^2 / \big| \frac{1}{2} + \frac{2Vq}{\log x} + it \big|^2 dt \big\|_q$ by $\max_{N \in \mathbb{Z}} \frac{1}{(|N|+1)^{1/4}} \big\| \int_{N-1/2}^{N+1/2} \big| F\big(\frac{1}{2} + \frac{2Vq}{\log x} + it\big) \big|^2 dt \big\|_q$, say. □

5. Proofs of the upper bounds in Theorems 1.1 and 1.2

In view of Proposition 4.1, the key to obtaining the upper bound in Theorem 1.1 will lie in proving the following. Recall here that $F_k(s)$ denotes the partial Euler product of $f(n)$ over $x^{e^{-(k+1)}}$-smooth numbers, and in the special case where $k=-1$ we usually write $F(s)$ (rather than $F_{-1}(s)$) for the partial Euler product over x-smooth numbers.

Key Proposition 5.1. *Let $f(n)$ be a Steinhaus random multiplicative function. For all large x, and uniformly for $1 \le q \le \log^{100} x$ (say) and $-1 \le k \le \mathcal{L} = \lfloor(\log\log x)/10\rfloor$ and $-e^k/\log x \le \sigma \le 1/(100\log(2q))$ (say), we have*

$$\mathbb{E}\left(\int_{-1/2}^{1/2}\left|F_k\left(\frac{1}{2}+\sigma+it\right)\right|^2 dt\right)^q \ll \frac{e^{O(q^2)}}{\log^{q-1} x}\left(\frac{\log x}{\log 2q}\right)^{q^2} \min\left\{\frac{1}{e^{k+1}}, \frac{1}{|\sigma|\log x}\right\}^{q^2-q+1}.$$

Key Proposition 5.1 is actually much more general, in terms of the allowed range of q and σ, than we immediately need (and the proof would let us extend the range of q quite a lot further if we wished, all it really requires is something like $e^k/\log x \le 1/(100\log(2q))$). The increased generality will be useful in Section 6, where Key Proposition 5.1 will play an auxiliary role, and also in clarifying the essential features of the proof.

Proof of the upper bound in Theorem 1.1, assuming Key Proposition 5.1. In view of the discussion in Section 3, it will suffice to prove the Theorem 1.1 upper bound for $1 \le q \le \log\log x$. And to do that, in view of Proposition 4.1 it will suffice to show that

$$\sum_{0\le k\le\mathcal{L}}\left\|\int_{-1/2}^{1/2}\left|F_k\left(\tfrac{1}{2}+\tfrac{q-k}{\log x}+it\right)\right|^2 dt\right\|_q^{1/2} \le e^{-(q/2)\log q-(q/2)\log\log(2q)+O(q)}\log^{q/2-1/2+1/2q} x.$$

Applying Key Proposition 5.1 with $\sigma = (q-k)/\log x$ (which is indeed $\le 1/(100\log(2q))$ on our range of q), we find the left-hand side is

$$\le \sum_{0\le k\le\mathcal{L}}\left(\frac{e^{O(q^2)}}{\log^{q-1} x}\left(\frac{\log x}{\log 2q}\right)^{q^2}\min\left\{\frac{1}{e^{k+1}}, \frac{1}{|q-k|}\right\}^{q^2-q+1}\right)^{1/2q}$$
$$= \sum_{0\le k\le\mathcal{L}}\left(e^{O(q^2)}\left(\frac{\log x}{\log 2q}\min\left\{\frac{1}{e^{k+1}}, \frac{1}{q}\right\}\right)^{q^2-q+1}\right)^{1/2q}.$$

It is easy to see that this satisfies our desired bound. □

For Theorem 1.2, we need a Rademacher analogue of the above.

Key Proposition 5.2. *Let $f(n)$ be a Rademacher random multiplicative function. For all large x, and uniformly for $1 \le q \le \log^{100} x$ (say) and $-1 \le k \le \mathcal{L} = \lfloor(\log\log x)/10\rfloor$ and $-e^k/\log x \le \sigma \le 1/(100\log(2q))$ (say), we have*

$$\mathbb{E}\Big(\int_{-1/2}^{1/2}\big|F_k\big(\tfrac{1}{2}+\sigma+it\big)\big|^2\,dt\Big)^q$$
$$\ll \frac{e^{O(q^2)}}{\log^q x}\Big(1+\min\Big\{\log\log x,\frac{1}{|q-q_0|}\Big\}\Big)\Big(\frac{\log x}{\log 2q}\Big)^{\max\{2q^2-q,q^2+1\}}\min\Big\{\frac{1}{e^{k+1}},\frac{1}{|\sigma|\log x}\Big\}^{\max\{2q^2-2q,q^2-q+1\}},$$

where $q_0=(1+\sqrt{5})/2$.

Furthermore, for any $|N|\geq 1$ *we have*

$$\mathbb{E}\Big(\int_{N-\frac{1}{2}}^{N+\frac{1}{2}}\big|F_k\big(\tfrac{1}{2}+\sigma+it\big)\big|^2\,dt\Big)^q$$
$$\ll \min\Big\{|N|^{1/100},\frac{\log x}{e^{k+1}\log 2q},\frac{1}{|\sigma|\log 2q}\Big\}^{q(q+1)}\frac{e^{O(q^2)}}{\log^{q-1}x}\Big(\frac{\log x}{\log 2q}\Big)^{q^2}\min\Big\{\frac{1}{e^{k+1}},\frac{1}{|\sigma|\log x}\Big\}^{q^2-q+1}.$$

Proof of the upper bound in Theorem 1.2, assuming Key Proposition 5.2. Similarly as in the Steinhaus case, in view of Proposition 4.2 and the discussion in Section 3 it will suffice to show that for all $1\leq q\leq\log\log x$, we have

$$\sum_{0\leq k\leq\mathcal{L}}\max_{N\in\mathbb{Z}}\frac{1}{(|N|+1)^{1/8}}\Big\|\int_{N-1/2}^{N+1/2}\Big|F_k\Big(\frac{1}{2}+\frac{q-k}{\log x}+it\Big)\Big|^2\,dt\Big\|_q^{1/2}$$
$$\leq e^{-q\log q-q\log\log(2q)+O(q)}\Big(1+\min\Big\{\log\log x,\frac{1}{|q-q_0|}\Big\}\Big)^{1/2q}(\log x)^{\max\{q-1,q/2-1/2+1/2q\}}.$$

We apply Key Proposition 5.2 with $\sigma=(q-k)/\log x$ (which is indeed $\leq 1/(100\log(2q))$ on our range of q). When $q\leq 15$, say, we have $\min\{|N|^{1/100},\log x/(e^{k+1}\log 2q),1/(|\sigma|\log 2q)\}^{q(q+1)}\leq |N|^{q/5}\leq|N|^{2q/8}$, so (on taking $2q$-th roots in Key Proposition 5.2 and then multiplying by the prefactor $1/(|N|+1)^{1/8}$) we see the contribution from $|N|\geq 1$ to $\max_{N\in\mathbb{Z}}$ will never exceed the contribution from the $N=0$ term. So overall, when $1\leq q\leq 15$ the left-hand side will be

$$\leq\sum_{0\leq k\leq\mathcal{L}}\Big(\frac{e^{O(q^2)}}{\log^q x}\min\Big\{\log\log x,\frac{1}{|q-q_0|}\Big\}\Big(\frac{\log x}{\log 2q}\Big)^{\max\{2q^2-q,q^2+1\}}\Big(\frac{1}{e^{k+1}}\Big)^{\max\{2q^2-2q,q^2-q+1\}}\Big)^{1/2q}$$
$$\ll\sum_{0\leq k\leq\mathcal{L}}\Big(\min\Big\{\log\log x,\frac{1}{|q-q_0|}\Big\}\Big(\frac{\log x}{e^{k+1}}\Big)^{\max\{2q(q-1),q^2-q+1\}}\Big)^{1/2q}.$$

This certainly gives our desired bound for $1\leq q\leq 15$.

When $15\leq q\leq\log\log x$, we note first that $\max\{2q^2-2q,q^2-q+1\}=2q^2-2q$. (In fact this is true as soon as $q\geq q_0$.) So using the bound

$$\min\Big\{|N|^{1/100},\frac{\log x}{e^{k+1}\log 2q},\frac{1}{|\sigma|\log 2q}\Big\}^{q(q+1)}\leq|N|^{(2q+1)/100}\min\Big\{\frac{\log x}{e^{k+1}\log 2q},\frac{1}{|\sigma|\log 2q}\Big\}^{q^2-q-1},$$

we again find that the contribution from $|N| \geq 1$ to $\max_{N\in\mathbb{Z}}$ will never exceed the contribution from the $N = 0$ term. Overall, in this case we get a bound

$$\ll \sum_{0\leq k\leq \mathcal{L}} \left(e^{O(q^2)} \left(\frac{\log x}{\log 2q} \min\left\{ \frac{1}{e^{k+1}}, \frac{1}{q} \right\} \right)^{2q^2-2q} \right)^{1/2q} \ll \left(e^{O(q^2)} \left(\frac{\log x}{q \log 2q} \right)^{2q^2-2q} \right)^{1/2q},$$

as desired. □

We shall prove Key Propositions 5.1 and 5.2 in several steps over the course of this section. For convenience in the writing we set $\mathcal{X} := \min\{\log x/e^{k+1}, 1/|\sigma|\}$, and note that under our hypotheses this is always $\geq 100\log(2q)$. The point of this definition is that the contribution from primes $p > e^{\mathcal{X}}$ in our Euler products will ultimately contribute only to the $e^{O(q^2)}$ term.

Preliminary maneuvres. We begin with a few manipulations to discretize and set up the problem, in both the Steinhaus and Rademacher cases. For any $q \geq 1$, we have

$$\begin{aligned} \left\| \int_{-1/2}^{1/2} \left|F_k\left(\tfrac{1}{2}+\sigma+it\right)\right|^2 dt \right\|_q &\leq \left\| \int_{-1/(2\mathcal{X})}^{1/(2\mathcal{X})} \sum_{|n|\leq \mathcal{X}/2+1} \left|F_k\left(\tfrac{1}{2}+\sigma+i\left(\tfrac{n}{\mathcal{X}}+t\right)\right)\right|^2 dt \right\|_q \\ &= \frac{1}{\mathcal{X}} \left\| \int_{-1/2\mathcal{X}}^{1/2\mathcal{X}} \mathcal{X} \sum_{|n|\leq \mathcal{X}/2+1} \left|F_k\left(\tfrac{1}{2}+\sigma+i\left(\tfrac{n}{\mathcal{X}}+t\right)\right)\right|^2 dt \right\|_q. \end{aligned}$$

Applying Hölder's inequality with exponent q to the normalized integral $\int_{-1/(2\mathcal{X})}^{1/(2\mathcal{X})} \mathcal{X}\, dt$, we see the right-hand side is

$$\leq \frac{1}{\mathcal{X}} \left(\int_{-1/(2\mathcal{X})}^{1/(2\mathcal{X})} \mathcal{X} \mathbb{E} \left(\sum_{|n|\leq \mathcal{X}/2+1} \left|F_k\left(\tfrac{1}{2}+\sigma+i\left(\tfrac{n}{\mathcal{X}}+t\right)\right)\right|^2 \right)^q dt \right)^{1/q}.$$

In the Steinhaus case, where $\left|F_k\left(\tfrac{1}{2}+\sigma+i\left(\tfrac{n}{\mathcal{X}}+t\right)\right)\right|^2$ has the same distribution for any given shift t, we can simplify the above to give the bound

$$\left\| \int_{-1/2}^{1/2} \left|F_k\left(\tfrac{1}{2}+\sigma+it\right)\right|^2 dt \right\|_q \leq \frac{1}{\mathcal{X}} \left\| \sum_{|n|\leq \mathcal{X}/2+1} \left|F_k\left(\tfrac{1}{2}+\sigma+\tfrac{in}{\mathcal{X}}\right)\right|^2 \right\|_q,$$

so we have indeed passed to studying a discrete sum rather than an integral. Finally, we rewrite the right-hand side as

$$\begin{aligned} &\frac{1}{\mathcal{X}} \left(\mathbb{E} \sum_{|n|\leq \mathcal{X}/2+1} \left|F_k\left(\tfrac{1}{2}+\sigma+\tfrac{in}{\mathcal{X}}\right)\right|^2 \left(\sum_{|m|\leq \mathcal{X}/2+1} \left|F_k\left(\tfrac{1}{2}+\sigma+\tfrac{im}{\mathcal{X}}\right)\right|^2 \right)^{q-1} \right)^{1/q} \\ &\qquad \ll \frac{1}{\mathcal{X}} \left(\mathcal{X} \mathbb{E} \left|F_k\left(\tfrac{1}{2}+\sigma\right)\right|^2 \left(\sum_{|m|\leq \mathcal{X}} \left|F_k\left(\tfrac{1}{2}+\sigma+\tfrac{im}{\mathcal{X}}\right)\right|^2 \right)^{q-1} \right)^{1/q}, \qquad (5\text{-}1) \end{aligned}$$

where the inequality again uses the distributional "translation invariance" (shifting n to zero in the outer sum, and replacing m by $m - n$ in the second sum).

In the case of Rademacher $f(n)$, if we mimic the above calculations we obtain that

$$\left\| \int_{N-1/2}^{N+1/2} \left|F_k\left(\tfrac{1}{2}+\sigma+it\right)\right|^2 dt \right\|_q$$
$$\leq \frac{1}{\mathcal{X}}\left(\int_{-1/2\mathcal{X}}^{1/2\mathcal{X}} \mathcal{X}\mathbb{E} \sum_{|n|\leq \mathcal{X}/2+1} \left|F_k\left(\tfrac{1}{2}+\sigma+i\left(\tfrac{n}{\mathcal{X}}+N+t\right)\right)\right|^2 \left(\sum_{|m|\leq \mathcal{X}/2+1} \left|F_k\left(\tfrac{1}{2}+\sigma+i\left(\tfrac{m}{\mathcal{X}}+N+t\right)\right)\right|^2 \right)^{q-1} dt \right)^{1/q}. \quad (5\text{-}2)$$

Proof of Key Proposition 5.1, for q ≥ 2. When $q \geq 2$, we are helped by the fact that we can use Hölder's inequality again to analyze $\left(\sum_{|m|\leq \mathcal{X}} \left|F_k\left(\frac{1}{2}+\sigma+\frac{im}{\mathcal{X}}\right)\right|^2\right)^{q-1}$ in (5-1). If we let $\mu := \sum_{|m|\leq \mathcal{X}} 1/(|m|+1)^2$, so that $\mu \asymp 1$, then first we have

$$\left(\sum_{|m|\leq \mathcal{X}} \left|F_k\left(\tfrac{1}{2}+\sigma+\tfrac{im}{\mathcal{X}}\right)\right|^2 \right)^{q-1} = \mu^{q-1}\left(\frac{1}{\mu} \sum_{|m|\leq \mathcal{X}} \frac{1}{(|m|+1)^2}(|m|+1)^2 \left|F_k\left(\tfrac{1}{2}+\sigma+\tfrac{im}{\mathcal{X}}\right)\right|^2 \right)^{q-1}.$$

Using Hölder's inequality with exponent $q-1$, we deduce

$$\begin{aligned} \left(\sum_{|m|\leq \mathcal{X}} \left|F_k\left(\tfrac{1}{2}+\sigma+\tfrac{im}{\mathcal{X}}\right)\right|^2 \right)^{q-1} &\leq \mu^{q-1}\cdot \frac{1}{\mu} \sum_{|m|\leq \mathcal{X}} \frac{1}{(|m|+1)^2}\left((|m|+1)^2 \left|F_k\left(\tfrac{1}{2}+\sigma+\tfrac{im}{\mathcal{X}}\right)\right|^2\right)^{q-1} \\ &= e^{O(q)} \sum_{|m|\leq \mathcal{X}} \frac{1}{(|m|+1)^2}(|m|+1)^{2(q-1)} \left|F_k\left(\tfrac{1}{2}+\sigma+\tfrac{im}{\mathcal{X}}\right)\right|^{2(q-1)}. \end{aligned} \quad (5\text{-}3)$$

We remark that the choice of weights $1/(|m|+1)^2$ that we introduced is fairly arbitrary. The key point is that we expect, in (5-1), that the only significant contribution should come from small m (for which $\left|F_k\left(\frac{1}{2}+\sigma+\frac{im}{\mathcal{X}}\right)\right|^2$ will be highly correlated with the outer term $\left|F_k\left(\frac{1}{2}+\sigma\right)\right|^2$), so we don't want to pick up a factor like $\mathcal{X}$ (inefficiently reflecting the total length of the sum) in our application of Hölder's inequality.

In view of the above computation, to bound the right-hand side of (5-1) when $q \geq 2$ we need to bound terms of the form

$$(|m|+1)^{2(q-1)}\mathbb{E}\left|F_k\left(\tfrac{1}{2}+\sigma\right)\right|^2 \left|F_k\left(\tfrac{1}{2}+\sigma+\tfrac{im}{\mathcal{X}}\right)\right|^{2(q-1)}.$$

Recall that $-e^k/\log x \leq \sigma \leq 1/100\log(2q)$ here. Inserting the definition of $F_k(s)$, and using a trivial bound $e^{O\left(\sum_{p\leq 100q^2} q/p^{1/2+\sigma}\right)} = e^{O\left(\sum_{p\leq 100q^2} q/\sqrt{p}\right)} = e^{O(q^2/\log q)}$ for the parts of the Euler products over primes $\leq 100q^2$, this is

$$e^{O(q^2/\log q)}(|m|+1)^{2(q-1)}\mathbb{E} \prod_{100q^2 < p \leq x^{e^{-(k+1)}}} \left|1-\frac{f(p)}{p^{1/2+\sigma}}\right|^{-2} \left|1-\frac{f(p)}{p^{1/2+\sigma+im/\mathcal{X}}}\right|^{-2(q-1)}.$$

Now if $e^{k+1}/\log x \leq \sigma \leq 1/100\log(2q)$, (and so $\mathcal{X} := \min\{\log x/e^{k+1}, 1/|\sigma|\} = 1/\sigma$), then the first part of Euler Product Result 2.1 implies that the expectation of the part of the Euler product over primes $e^{1/\sigma} < p \leq x^{e^{-(k+1)}}$ is equal to $\exp\{O(\sum_{e^{1/\sigma} < p \leq x^{e^{-(k+1)}}} q^2/p^{1+2\sigma} + q^3/e^{1/2\sigma})\}$, which is all $e^{O(q^2)}$. Using this fact, as well as the independence of $f(p)$ for different primes p, we find the above is always equal to

$$e^{O(q^2)}(|m|+1)^{2(q-1)}\mathbb{E}\prod_{100q^2<p\le e^{\mathcal{X}}}\left|1-\frac{f(p)}{p^{1/2+\sigma}}\right|^{-2}\left|1-\frac{f(p)}{p^{1/2+\sigma+im/\mathcal{X}}}\right|^{-2(q-1)}.$$

Notice that our size assumptions on σ, k, q guarantee that $e^{\mathcal{X}}$ is larger than $100q^2$. Finally, the second part of Euler Product Result 2.1 implies this is all equal to

$$e^{O(q^2)}(|m|+1)^{2(q-1)}\left(\frac{\mathcal{X}}{\log q}\right)^{1+(q-1)^2}\left(1+\frac{\mathcal{X}}{(|m|+1)\log q}\right)^{2(q-1)}=e^{O(q^2)}\left(\frac{\mathcal{X}}{\log q}\right)^{q^2}.$$

Putting this together with (5-3) and (5-1), we find

$$\left\|\int_{-1/2}^{1/2}\left|F_k\left(\tfrac12+\sigma+it\right)\right|^2dt\right\|_q\ll\frac{1}{\mathcal{X}}\left(\mathcal{X}\cdot e^{O(q^2)}\sum_{|m|\le\mathcal{X}}\frac{1}{(|m|+1)^2}\left(\frac{\mathcal{X}}{\log q}\right)^{q^2}\right)^{1/q}$$
$$=\frac{1}{\mathcal{X}}\left(\mathcal{X}\cdot e^{O(q^2)}\left(\frac{\mathcal{X}}{\log q}\right)^{q^2}\right)^{1/q}.$$

Raising everything to the power q and inserting the fact that $\mathcal{X}=\min\{\log x/e^{k+1}, 1/|\sigma|\}$, this gives the statement of Key Proposition 5.1. □

Proof of Key Proposition 5.2, for q ≥ 2. We begin with the second part of Key Proposition 5.2, where $|N|\ge 1$. Then similarly as in the deduction of (5-3) in the Steinhaus case, for any $|n|\le\mathcal{X}/2+1$ and any $|t|\le 1/(2\mathcal{X})$ we can use Hölder's inequality to show

$$\left(\sum_{|m|\le\frac{\mathcal{X}}{2}+1}\left|F_k\left(\tfrac12+\sigma+i\left(\tfrac{m}{\mathcal{X}}+N+t\right)\right)\right|^2\right)^{q-1}$$
$$\le e^{O(q)}\sum_{|m|\le\frac{\mathcal{X}}{2}+1}\frac{1}{(|m-n|+1)^2}(|m-n|+1)^{2(q-1)}\left|F_k\left(\tfrac12+\sigma+i\left(\tfrac{m}{\mathcal{X}}+N+t\right)\right)\right|^{2(q-1)}.$$

So to bound the right-hand side of (5-2), we need to bound terms of the form

$$(|m-n|+1)^{2(q-1)}\mathbb{E}\left|F_k\left(\tfrac12+\sigma+i\left(\tfrac{n}{\mathcal{X}}+N+t\right)\right)\right|^2\left|F_k\left(\tfrac12+\sigma+i\left(\tfrac{m}{\mathcal{X}}+N+t\right)\right)\right|^{2(q-1)}.$$

As in the Steinhaus case, the contribution from primes $p\le 100q^2$ to this expectation is trivially $e^{O(q^2/\log q)}$. Using the first part of Euler Product Result 2.2, the contribution from primes $e^{\mathcal{X}}<p\le x^{e^{-(k+1)}}$ is $e^{O(q^2)}$, and overall (noting that the imaginary shifts $n/\mathcal{X}+N+t, m/\mathcal{X}+N+t$ are $\gg|N|\gg 1$ and also $\ll|N|$) the above expression is at most

$$e^{O(q^2)}\min\left\{\frac{\mathcal{X}}{\log q}, |N|^{\frac{1}{100}}\right\}^{(q-1)^2+3(q-1)}(|m-n|+1)^{2(q-1)}\left(\frac{\mathcal{X}}{\log q}\right)^{1+(q-1)^2}\left(\frac{\mathcal{X}}{(|m-n|+1)\log q}\right)^{2(q-1)}.$$

Apart from the factor $\min\{\mathcal{X}/\log q, |N|^{1/100}\}^{(q-1)(q+2)}$, this is precisely analogous to the estimate we had in the Steinhaus case, so when $|N|\ge 1$ we indeed get the same bound as in the Steinhaus case apart from a multiplier

$$\min\left\{\frac{\mathcal{X}}{\log q}, |N|^{1/100}\right\}^{(q-1)(q+2)} \le \min\left\{\frac{\mathcal{X}}{\log q}, |N|^{1/100}\right\}^{q(q+1)} = \min\left\{\frac{\log x}{e^{k+1}\log q}, \frac{1}{|\sigma|\log q}, |N|^{1/100}\right\}^{q(q+1)}.$$

It remains to address the first part of Key Proposition 5.2, where $N=0$. In this case, when $q \ge 2$ we expect the main contribution to (5-2) to come from terms with $n, m \approx 0$, so rather than splitting up the sum over m according to the size of $|m-n|$ we shall just split it up according to the size of m. Proceeding in this way, using Hölder's inequality as in the Steinhaus case we find for any $|t| \le 1/(2\mathcal{X})$ that

$$\sum_{|n|\le \frac{\mathcal{X}}{2}+1} \left|F_k\left(\tfrac{1}{2}+\sigma+i\left(\tfrac{n}{\mathcal{X}}+t\right)\right)\right|^2 \left(\sum_{|m|\le \mathcal{X}/2+1} \left|F_k\left(\tfrac{1}{2}+\sigma+i\left(\tfrac{m}{\mathcal{X}}+t\right)\right)\right|^2\right)^{q-1}$$
$$\le e^{O(q)} \sum_{|n|\le \mathcal{X}/2+1} \left|F_k\left(\tfrac{1}{2}+\sigma+i\left(\tfrac{n}{\mathcal{X}}+t\right)\right)\right|^2 \sum_{|m|\le \mathcal{X}/2+1} \frac{1}{(|m|+1)^2}(|m|+1)^{2(q-1)}\left|F_k\left(\tfrac{1}{2}+\sigma+i\left(\tfrac{m}{\mathcal{X}}+t\right)\right)\right|^{2(q-1)}. \quad (5\text{-}4)$$

So to bound the right-hand side of (5-2), we again need to bound terms of the form

$$(|m|+1)^{2(q-1)}\mathbb{E}\left|F_k\left(\tfrac{1}{2}+\sigma+i\left(\tfrac{n}{\mathcal{X}}+t\right)\right)\right|^2\left|F_k\left(\tfrac{1}{2}+\sigma+i\left(\tfrac{m}{\mathcal{X}}+t\right)\right)\right|^{2(q-1)}.$$

Using the second part of Euler Product Result 2.2, this is

$$e^{O(q^2)}(|m|+1)^{2(q-1)}\left(1+\frac{\mathcal{X}}{(|m|+1)\log q}\right)^{(q-1)^2-(q-1)}\left(\frac{\mathcal{X}}{\log q}\right)^{1+(q-1)^2} \cdot\left(\left(1+\frac{\mathcal{X}}{(|m-n|+1)\log q}\right)\left(1+\frac{\mathcal{X}}{(|m+n|+1)\log q}\right)\right)^{2(q-1)}.$$

Now depending on the signs of m, n, one of the terms $|m-n|$, $|m+n|$ will be equal to $\big||m|-|n|\big|$ and the other will equal $|m|+|n| \ge |m|$. So the above is always

$$\le e^{O(q^2)}(|m|+1)^{2(q-1)}\left(1+\frac{\mathcal{X}}{(|m|+1)\log q}\right)^{q(q-1)}\left(\frac{\mathcal{X}}{\log q}\right)^{1+(q-1)^2}\left(\frac{\mathcal{X}}{\left(\big||m|-|n|\big|+1\right)\log q}\right)^{2(q-1)}.$$

Putting this together with (5-4) and (5-2), if we first perform the sum over $|n| \le \mathcal{X}/2+1$ we get that $\left\| \int_{-1/2}^{1/2} \left|F_k\left(\tfrac{1}{2}+\sigma+it\right)\right|^2 dt\right\|_q$ is at most

$$\frac{e^{O(q)}}{\mathcal{X}}\left(\sum_{|m|\le \mathcal{X}/2+1} \frac{(|m|+1)^{2(q-1)}}{(|m|+1)^2}\left(1+\frac{\mathcal{X}}{(|m|+1)\log q}\right)^{q(q-1)}\left(\frac{\mathcal{X}}{\log q}\right)^{1+(q-1)^2+2(q-1)}\right)^{1/q}.$$

Finally performing the sum over m, the dominant contribution comes from small terms (note that for terms with $|m| > \mathcal{X}/\log q$ we have $(1+\mathcal{X}/((|m|+1)\log q))^{q(q-1)} = e^{O(q^2)}$, so overall these contribute at most $e^{O(q^2)}\mathcal{X}^{2q-3}(\mathcal{X}/\log q)^{1+(q-1)^2+2(q-1)} = e^{O(q^2)}(\mathcal{X}/\log q)^{q^2+2q-3}$ inside the bracket), and gives us a bound $\ll [e^{O(q)}/\mathcal{X}](\mathcal{X}/\log q)^{(2q^2-q)/q}$. Raising everything to the power $q \ge 2$ and inserting the fact that $\mathcal{X} = \min\{\log x/e^{k+1}, 1/|\sigma|\}$, this gives the bound claimed in Key Proposition 5.2. ☐

Proof of Key Proposition 5.1, for $1 < q < 2$. When $1 < q < 2$, it is not immediately obvious how to analyze the term $\mathbb{E}\big|F_k\big(\tfrac12+\sigma\big)\big|^2\big(\sum_{|m|\le\mathcal{X}}\big|F_k\big(\tfrac12+\sigma+\tfrac{im}{\mathcal{X}}\big)\big|^2\big)^{q-1}$ in (5-1). We may begin by letting $C=C(q)=e^{1/(q-1)}$, and noting that $\mathbb{E}\big|F_k\big(\tfrac12+\sigma\big)\big|^2\big(\sum_{|m|\le\mathcal{X}}\big|F_k\big(\tfrac12+\sigma+\tfrac{im}{\mathcal{X}}\big)\big|^2\big)^{q-1}$ is

$$\le \mathbb{E}\big|F_k\big(\tfrac12+\sigma\big)\big|^2\Bigg(\sum_{d\le(q-1)\log\mathcal{X}+1}\ \sum_{C^{d-1}\le|m|\le C^d}\big|F_k\big(\tfrac12+\sigma+\tfrac{im}{\mathcal{X}}\big)\big|^2\Bigg)^{q-1}.$$

Here we adopt the convention that the term $m=0$ is included in $\sum_{C^{d-1}\le|m|\le C^d}$ when $d=1$, and that any terms with $|m|>\mathcal{X}$ are omitted from all sums (so the imaginary shift in the second copy of F_k always has size $|m/\mathcal{X}|\le 1$). The motivation for splitting things up like this is that we expect our estimates for all terms with $\sum_{C^{d-1}\le|m|\le C^d}$ to be roughly the same, up to a factor $C^{O(1)}$. And, when everything is raised to the power $q-1$, this factor simply becomes a constant multiplier. Next, if we let $D=D(q)\in\mathbb{N}$ be a parameter, to be fixed later, we can split things up further and find

$$\begin{aligned}
&\mathbb{E}\big|F_k\big(\tfrac12+\sigma\big)\big|^2\Bigg(\sum_{|m|\le\mathcal{X}}\big|F_k\big(\tfrac12+\sigma+\tfrac{im}{\mathcal{X}}\big)\big|^2\Bigg)^{q-1}\\
&\quad\le \sum_{r\le(q-1)\log\mathcal{X}/D+1}\mathbb{E}\big|F_k\big(\tfrac12+\sigma\big)\big|^2\Bigg(\sum_{(r-1)D<d\le rD}\ \sum_{C^{d-1}\le|m|\le C^d}\big|F_k\big(\tfrac12+\sigma+\tfrac{im}{\mathcal{X}}\big)\big|^2\Bigg)^{q-1}\\
&\quad\ll D^{q-1}\sum_{r\le(q-1)\log\mathcal{X}/D+1}\mathbb{E}\max_{(r-1)D<d\le rD}\big|F_k\big(\tfrac12+\sigma\big)\big|^2\Bigg(\sum_{C^{d-1}\le|m|\le C^d}\big|F_k\big(\tfrac12+\sigma+\tfrac{im}{\mathcal{X}}\big)\big|^2\Bigg)^{q-1}. \qquad (5\text{-}5)
\end{aligned}$$

Notice that we may further assume that all terms d for which $C^{d-1}>\mathcal{X}$ are omitted here, since for those the sum over m is empty (by our earlier convention).

Now in the sum over m, we expect (thinking about Euler Product Result 2.1) that the part of the Euler product $F_k\big(\tfrac12+\sigma+\tfrac{im}{\mathcal{X}}\big)$ on primes $\le e^{\mathcal{X}/C^d}$ will be roughly the same size for all $C^{d-1}\le|m|\le C^d$, and indeed roughly the same size as the corresponding part of $F_k\big(\tfrac12+\sigma\big)$. To simplify our writing about this, for each $d\ge1$ and $|m|\le\mathcal{X}$ let us set

$$G_d(m):=\prod_{p\le e^{\mathcal{X}/C^d}}\left|1-\frac{f(p)}{p^{1/2+\sigma+im/\mathcal{X}}}\right|^{-2},\quad\text{and}\quad H_d(m):=\frac{\big|F_k\big(\tfrac12+\sigma+\tfrac{im}{\mathcal{X}}\big)\big|^2}{G_d(m)}.$$

(These quantities of course depend on x,k,σ as well, but we suppress that in our notation.) We will also set $G_d:=G_d(0)$ and $H_d:=H_d(0)$. Then the expectation in (5-5) may be written as

$$\mathbb{E}\max_{(r-1)D<d\le rD}G_dH_d\Bigg(\sum_{C^{d-1}\le|m|\le C^d}G_d(m)H_d(m)\Bigg)^{q-1}.$$

We want to apply Hölder's inequality to this expectation, in such a way that the bracketed sum is raised to the power $1/(q-1)$, and so we can connect up the expectation with the terms inside. Prior to doing this, we rewrite the expectation again as

$$\mathbb{E} \max_{(r-1)D<d\le rD} G_d^{1-(q-1)^2} H_d^{1-(q-1)} C^{2(q-1)(2-q)d} \left(\frac{G_d^{q-1} H_d}{C^{2(2-q)d}} \sum_{C^{d-1}\le|m|\le C^d} G_d(m) H_d(m) \right)^{q-1}.$$

Simplifying the various exponents, this is all

$$\le \mathbb{E}\left(\max_{(r-1)D<d\le rD} G_d^{q(2-q)} H_d^{2-q} C^{2(q-1)(2-q)d} \right) \left(\max_{(r-1)D<d\le rD} \frac{G_d^{q-1} H_d}{C^{2(2-q)d}} \sum_{C^{d-1}\le|m|\le C^d} G_d(m) H_d(m) \right)^{q-1},$$

and now using Hölder's inequality with exponents $1/(2-q)$ and $1/(q-1)$, we get a bound

$$\le \left(\mathbb{E} \max_{(r-1)D<d\le rD} G_d^q H_d C^{2(q-1)d} \right)^{2-q} \left(\mathbb{E} \max_{(r-1)D<d\le rD} \frac{G_d^{q-1} H_d}{C^{2(2-q)d}} \sum_{C^{d-1}\le|m|\le C^d} G_d(m) H_d(m) \right)^{q-1}$$

$$\le \left(\mathbb{E} \max_{(r-1)D<d\le rD} G_d^q H_d C^{2(q-1)d} \right)^{2-q} \left(\sum_{(r-1)D<d\le rD} \mathbb{E} \frac{G_d^{q-1} H_d}{C^{2(2-q)d}} \sum_{C^{d-1}\le|m|\le C^d} G_d(m) H_d(m) \right)^{q-1}.$$

We remark that the motivation for the uneven splitting of the Euler products here (moving $G_d^{(q-1)^2}$ and H_d^{q-1} into the second bracket) is that, as noted above, $\mathbb{E} G_d^{q-1} G_d(m)$ will behave in approximately the same way as $\mathbb{E} G_d^q$, but on the large primes the shifts $im/\mathcal{X}$ provide extra cancellation in $\mathbb{E} H_d H_d(m)$. So the best way to split up the G_d terms is "evenly", i.e., such that the total exponent of G_d terms in both brackets after Hölder's inequality remains q, whereas for the H_d terms it is better to move a larger piece inside the second bracket (with the sum over m) to maximize the cancellation we pick up. As we shall see, the powers of C that we have introduced will serve to balance the final sizes of all the terms.

Using the independence of $f(p)$ for different primes, together with Euler Product Result 2.1, the sums inside the second bracket are

$$\sum_{(r-1)D<d\le rD} \frac{1}{C^{2(2-q)d}} \sum_{C^{d-1}\le|m|\le C^d} \mathbb{E} G_d^{q-1} G_d(m) \mathbb{E} H_d H_d(m)$$

$$\ll \sum_{(r-1)D<d\le rD} \frac{1}{C^{2(2-q)d}} \sum_{C^{d-1}\le|m|\le C^d} \left(1 + \frac{\mathcal{X}}{C^d}\right)^{1+(q-1)^2} \left(\frac{\mathcal{X}}{1+|m|}\right)^{2(q-1)} (\min\{\mathcal{X}, C^d\})^2 \left(\frac{\min\{\mathcal{X}, C^d\}}{1+|m|}\right)^2$$

$$\ll \sum_{(r-1)D<d\le rD} \frac{C^{O(1)}}{C^{2(2-q)d}} \mathcal{X}^{q^2} C^{(3-q^2)d}$$

$$= C^{O(1)} \mathcal{X}^{q^2} \sum_{(r-1)D<d\le rD} C^{-(q-1)^2 d} = C^{O(1)} \mathcal{X}^{q^2} C^{-(q-1)^2 (r-1)D}.$$

When performing this calculation, we noted that the contribution to $\mathbb{E} H_d H_d(m)$ from primes $p > e^{\mathcal{X}}$ is uniformly bounded (by the first part of Euler Product Result 2.1), similarly as in our analysis of the case $q \ge 2$. Some of our estimates here were a bit crude, but there seems to be no way to avoid losing some factors $C^{O(1)}$, which further explains why our choice of $C = e^{1/(q-1)}$ is essentially the largest we can make without incurring unacceptable losses.

To bound $\mathbb{E}\max_{(r-1)D<d\le rD} G_d^q H_d C^{2(q-1)d}$, where we need to handle the maximum in a nontrivial way rather than replacing it by a sum (because this term will not be raised to the small power $q-1$), we will use Probability Result 2.5. To do this, we first rewrite $\mathbb{E}\max_{(r-1)D<d\le rD} G_d^q H_d C^{2(q-1)d}$ as

$$\mathbb{E}\big|F_k\big(\tfrac{1}{2}+\sigma\big)\big|^2 \max_{(r-1)D<d\le rD} (G_d C^{2d})^{q-1} \\ = \mathbb{E}\big|F_k\big(\tfrac{1}{2}+\sigma\big)\big|^2 \tilde{\mathbb{E}} \max_{(r-1)D<d\le rD} \prod_{p\le e^{\mathcal{X}/C^d}} \left|1-\frac{f(p)}{p^{1/2+\sigma}}\right|^{-2(q-1)} C^{2(q-1)d},$$

where $\tilde{\mathbb{E}}$ is expectation under the "tilted" measure defined by $\tilde{\mathbb{P}}(A) = \mathbb{E}\big|F_k\big(\tfrac{1}{2}+\sigma\big)\big|^2 \mathbf{1}_A / \mathbb{E}\big|F_k\big(\tfrac{1}{2}+\sigma\big)\big|^2$ for each event A (and $\mathbf{1}$ denotes the indicator function). We note, for use in a little while, that if A is an event not involving certain primes then those terms factor out from the expectation and cancel between numerator and denominator in the definition of $\tilde{\mathbb{P}}(A)$. Furthermore, the random variables $f(p)$ are still independent under the measure $\tilde{\mathbb{P}}$, since if A, B are events involving disjoint sets of primes then we can split up the Euler product $\big|F_k\big(\tfrac{1}{2}+\sigma\big)\big|^2$ into subproducts over the corresponding sets, and then the expectation $\mathbb{E}$ will split up correspondingly.

Now Euler Product Result 2.1 implies that $\mathbb{E}\big|F_k\big(\tfrac{1}{2}+\sigma\big)\big|^2 \asymp \mathcal{X}$. Furthermore, if we write

$$L_d := \prod_{p\le e^{\mathcal{X}/C^d}} \left|1-\frac{f(p)}{p^{1/2+\sigma}}\right|^{-2(q-1)/1.01}$$

(say), and $\lambda_d := \tilde{\mathbb{E}} L_d$, then Euler Product Result 2.1 and the independence of the $f(p)$ imply that

$$\lambda_d = \frac{\mathbb{E}\prod_{p\le e^{\mathcal{X}/C^d}} |1-f(p)/p^{1/2+\sigma}|^{-2(1+(q-1)/1.01)}}{\mathbb{E}\prod_{p\le e^{\mathcal{X}/C^d}} |1-f(p)/p^{1/2+\sigma}|^{-2}} \asymp \left(1+\frac{\mathcal{X}}{C^d}\right)^{2(q-1)/1.01+(q-1)^2/1.01^2}.$$

We similarly get that $\tilde{\mathbb{E}} L_d^{1.01} \asymp (1+\mathcal{X}/C^d)^{2(q-1)+(q-1)^2}$. So we have shown that

$$\mathbb{E}\max_{(r-1)D<d\le rD} G_d^q H_d C^{2(q-1)d} \asymp \mathcal{X}\cdot \tilde{\mathbb{E}} \max_{(r-1)D<d\le rD} \left(\frac{L_d}{\lambda_d}\right)^{1.01} (C^d+\mathcal{X})^{2(q-1)} \left(1+\frac{\mathcal{X}}{C^d}\right)^{(q-1)^2/1.01} \\ \ll \mathcal{X}^{1+2(q-1)} \left(1+\frac{\mathcal{X}}{C^{(r-1)D+1}}\right)^{(q-1)^2/1.01} \tilde{\mathbb{E}} \max_{(r-1)D<d\le rD} \left(\frac{L_d}{\lambda_d}\right)^{1.01},$$

where we used the fact that $C^d \le C\mathcal{X}$ (given our convention that those d for which $C^{d-1} > \mathcal{X}$ are omitted) and $C^{2(q-1)} \ll 1$. Finally, since the $f(p)$ are independent under the measure $\tilde{\mathbb{P}}$ (and so the "increments" of different primes in the Euler product are independent), the sequence of random variables $(L_{rD}/\lambda_{rD}), (L_{rD-1}/\lambda_{rD-1}), \ldots, (L_{(r-1)D+1}/\lambda_{(r-1)D+1})$ (taken in that order) form a nonnegative submartingale relative to $\tilde{\mathbb{P}}$ and to the sigma algebras generated by $(f(p))_{p\le e^{\mathcal{X}/C^{rD}}}$, $(f(p))_{p\le e^{\mathcal{X}/C^{rD-1}}}, \ldots,$ $(f(p))_{p\le e^{\mathcal{X}/C^{(r-1)D+1}}}$. For example, we may calculate the conditional expectation

$$\tilde{\mathbb{E}}\biggl(\biggl(\frac{L_{rD-1}}{\lambda_{rD-1}}\biggr) \mid (f(p))_{p\le e^{\mathcal{X}/C^{rD}}}\biggr) = \frac{L_{rD}}{\lambda_{rD-1}}\tilde{\mathbb{E}}\biggl(\prod_{e^{\mathcal{X}/C^{rD}}<p\le e^{\mathcal{X}/C^{rD-1}}}\biggl|1-\frac{f(p)}{p^{1/2+\sigma}}\biggr|^{-2(q-1)/1.01} \mid (f(p))_{p\le e^{\mathcal{X}/C^{rD}}}\biggr)$$
$$= \frac{L_{rD}}{\lambda_{rD-1}}\tilde{\mathbb{E}}\biggl(\prod_{e^{\mathcal{X}/C^{rD}}<p\le e^{\mathcal{X}/C^{rD-1}}}\biggl|1-\frac{f(p)}{p^{1/2+\sigma}}\biggr|^{-2(q-1)/1.01}\biggr)$$
$$= \frac{L_{rD}}{\lambda_{rD}},$$

which gives the "nondecreasing on average" property from the definition of a submartingale. Thus Probability Result 2.5 is applicable, and gives that $\tilde{\mathbb{E}}\max_{(r-1)D<d\le rD}(L_d/\lambda_d)^{1.01}$ is

$$\ll \tilde{\mathbb{E}}\biggl(\frac{L_{(r-1)D+1}}{\lambda_{(r-1)D+1}}\biggr)^{1.01} \asymp \frac{\bigl(1+\frac{\mathcal{X}}{C^{(r-1)D+1}}\bigr)^{2(q-1)+(q-1)^2}}{\lambda_{(r-1)D+1}^{1.01}} \asymp \biggl(1+\frac{\mathcal{X}}{C^{(r-1)D+1}}\biggr)^{(q-1)^2-\frac{(q-1)^2}{1.01}}.$$

Putting together (5-1), (5-5), and the above calculations, we get that

$$\biggl\|\int_{-1/2}^{1/2}\Bigl|F_k\bigl(\tfrac12+\sigma+it\bigr)\Bigr|^2\,dt\biggr\|_q$$
$$\ll \frac{1}{\mathcal{X}}\biggl(\mathcal{X}D^{q-1}\sum_{r\le((q-1)\log\mathcal{X})/D+1}\biggl(\frac{\mathcal{X}^{q^2}}{C^{(r-1)D(q-1)^2}}\biggr)^{2-q}(C^{O(1)}\mathcal{X}^{q^2}C^{-(q-1)^2(r-1)D})^{q-1}\biggr)^{1/q}.$$

Recalling that $C=e^{1/(q-1)}$ and collecting terms together, we find this is all

$$\ll \tfrac{1}{\mathcal{X}}\biggl(\mathcal{X}^{1+q^2}D^{q-1}\sum_{r\le(q-1)\log\mathcal{X}/D+1}C^{-(r-1)D(q-1)^2}\biggr)^{1/q} = \tfrac{1}{\mathcal{X}}\biggl(\mathcal{X}^{1+q^2}D^{q-1}\sum_{r\le(q-1)\log\mathcal{X}/D+1}e^{-(r-1)D(q-1)}\biggr)^{1/q}.$$

So if we finally choose $D:=\lfloor 1/(q-1)\rfloor$, then both the sum over r and the term D^{q-1} will be $\ll 1$. Recalling that $\mathcal{X}=\min\{(\log x)/e^{k+1}, 1/|\sigma|\}$, we see this bound is as claimed in Key Proposition 5.1. □

***Proof of Key Proposition 5.2, for* $1<q<2$.** We again begin with the second part of the proposition, where $|N|\ge 1$. In this case we can analyze the terms $\mathbb{E}\bigl|F_k(\frac12+\sigma+i(\frac{n}{\mathcal{X}}+N+t))\bigr|^2\bigl(\sum_{|m|\le\frac{\mathcal{X}}{2}+1}\bigl|F_k\bigl(\frac12+\sigma+i\bigl(\frac{m}{\mathcal{X}}+N+t\bigr)\bigr)\bigr|^2\bigr)^{q-1}$ in (5-2) by splitting the sum over m into subsums where $C^{d-1}\le|m-n|\le C^d$, and otherwise following the argument from the Steinhaus case. We obtain the same estimates as there, except the error term in Euler Product Result 2.2 produces an additional factor

$$\min\bigl\{1+\tfrac{\mathcal{X}}{C^d}, |N|^{1/100}\bigr\}^{|(q-1)^2-(q-1)|+4(q-1)}\min\biggl\{C^d, \mathcal{X}, 1+\frac{|N|^{1/100}}{1+\mathcal{X}/C^d}\biggr\}^4 \ll \min\{\mathcal{X}, |N|^{1/100}\}^4$$

when estimating (the analogue of) the terms $\mathbb{E}G_d^{q-1}G_d(m)\mathbb{E}H_dH_d(m)$, and an additional factor $\min\{1+\mathcal{X}/C^{(r-1)D+1}, |N|^{1/100}\}^{q(q-1)} \ll \min\{\mathcal{X}, |N|^{1/100}\}^{q(q-1)}$ when estimating (the analogue of) the term $\mathbb{E}\max_{(r-1)D<d\le rD}G_d^qH_dC^{2(q-1)d}$. So overall we get the same bound as in the Steinhaus case, apart from

a factor

$$(\min\{\mathcal{X}, |N|^{1/100}\}^{q(q-1)})^{2-q}(\min\{\mathcal{X}, |N|^{1/100}\}^4)^{(q-1)} \ll \min\{\mathcal{X}, |N|^{1/100}\}^{(q-1)(4+2q-q^2)}.$$

A small calculation shows that for $1 \le q \le 2$, we have $(q-1)(4+2q-q^2) \le 5(q-1) \le q(q+1)$, giving the factor $\min\{\mathcal{X}, |N|^{1/100}\}^{q(q+1)} = \min\{(\log x)/e^{k+1}, 1/|\sigma|, |N|^{1/100}\}^{q(q+1)}$ claimed in the second part of Key Proposition 5.2.

When $N = 0$, to prove Key Proposition 5.2 we need to bound

$$\sum_{|n|\le \mathcal{X}/2+1} \mathbb{E}\left|F_k\left(\tfrac{1}{2}+\sigma+i\left(\tfrac{n}{\mathcal{X}}+t\right)\right)\right|^2 \left(\sum_{|m|\le \mathcal{X}/2+1} \left|F_k\left(\tfrac{1}{2}+\sigma+i\left(\tfrac{m}{\mathcal{X}}+t\right)\right)\right|^2\right)^{q-1}$$

in (5-2). Following the same argument that led to the bound (5-5) in the Steinhaus case, but now splitting the sum over m according to the size of $|m|-|n|$ rather than the size of $|m|$, one obtains that

$$\begin{aligned}\sum_{|n|\le \mathcal{X}/2+1} \mathbb{E}\left|F_k\left(\tfrac{1}{2}+\sigma+i\left(\tfrac{n}{\mathcal{X}}+t\right)\right)\right|^2 &\left(\sum_{|m|\le \mathcal{X}/2+1} \left|F_k\left(\tfrac{1}{2}+\sigma+i\left(\tfrac{m}{\mathcal{X}}+t\right)\right)\right|^2\right)^{q-1} \\ &\ll D^{q-1} \sum_{|n|\le \mathcal{X}/2+1} \sum_{r\le (q-1)\log \mathcal{X}/D+1} \mathbb{E} \max_{(r-1)D<d\le rD} \left|F_k\left(\tfrac{1}{2}+\sigma+i\left(\tfrac{n}{\mathcal{X}}+t\right)\right)\right|^2 \\ &\qquad \cdot \left(\sum_{\substack{|m|\le \mathcal{X}/2+1,\\ C^{d-1}\le ||m|-|n||\le C^d}} \left|F_k\left(\tfrac{1}{2}+\sigma+i\left(\tfrac{m}{\mathcal{X}}+t\right)\right)\right|^2\right)^{q-1}. \quad (5\text{-}6)\end{aligned}$$

Here we again have $C = e^{1/(q-1)}$, and $D = D(q) \in \mathbb{N}$ is a parameter, and we adopt our usual conventions (analogously to the Steinhaus case) about including the $|m| = |n|$ term when $d = 1$ and omitting overly large terms from all sums.

Now for each $d \ge 1$ and $|m| \le \mathcal{X}/2+1$, and treating t as fixed, we shall set

$$G_d(m) := \prod_{p\le e^{\mathcal{X}/C^d}} \left|1+\frac{f(p)}{p^{1/2+\sigma+i(m/\mathcal{X}+t)}}\right|^2, \quad \text{and} \quad H_d(m) := \frac{\left|F_k\left(\frac{1}{2}+\sigma+i\left(\frac{m}{\mathcal{X}}+t\right)\right)\right|^2}{G_d(m)}.$$

This is the same notation that we used in the Steinhaus case, but with the Euler products now replaced by their Rademacher versions (supported on squarefree numbers only). Splitting the expectation and applying Hölder's inequality as in the Steinhaus case, it follows that (5-6) is

$$\begin{aligned}\ll D^{q-1} \sum_{|n|\le \mathcal{X}/2+1} \sum_{r\le (q-1)\log \mathcal{X}/D+1} &\left(\mathbb{E} \max_{(r-1)D<d\le rD} G_d(n)^q H_d(n) C^{2(q-1)d}\right)^{2-q} \\ &\cdot \left(\sum_{(r-1)D<d\le rD} \mathbb{E}\frac{G_d(n)^{q-1}H_d(n)}{C^{2(2-q)d}} \sum_{\substack{|m|\le \mathcal{X}/2+1,\\ C^{d-1}\le ||m|-|n||\le C^d}} G_d(m)H_d(m)\right)^{q-1}.\end{aligned}$$

Continuing to follow the argument from the Steinhaus case, but using Euler Product Result 2.2 in place of Euler Product Result 2.1, we can bound these terms further. Proceeding to do this, and noting that one of the terms $|m-n|$, $|m+n|$ that arise in Euler Product Result 2.2 will always equal $\big||m|-|n|\big|$ and the other will equal $|m|+|n| \geq |n|$, we find the sums in the second bracket are

$$\sum_{(r-1)D<d\leq rD} \frac{1}{C^{2(2-q)d}} \sum_{\substack{|m|\leq \mathcal{X}/2+1, \\ C^{d-1}\leq ||m|-|n||\leq C^d}} \mathbb{E} G_d(n)^{q-1} G_d(m) \mathbb{E} H_d(n) H_d(m)$$

$$\ll \sum_{(r-1)D<d\leq rD} \frac{1}{C^{2(2-q)d}} \sum_{C^{d-1}\leq ||m|-|n||\leq C^d} \min\left\{\frac{\mathcal{X}}{C^d}, \frac{\mathcal{X}}{|n|}\right\}^{(q-1)^2-(q-1)} \left(1+\frac{\mathcal{X}}{C^d}\right)^{1+(q-1)^2}$$
$$\cdot \left(\frac{\mathcal{X}}{1+\big||m|-|n|\big|} \min\left\{\frac{\mathcal{X}}{C^d}, \frac{\mathcal{X}}{|n|}\right\}\right)^{2(q-1)} (\min\{\mathcal{X}, C^d\})^2 \left(\frac{\min\{\mathcal{X}, C^d\}}{1+\big||m|-|n|\big|}\left(1+\frac{\min\{\mathcal{X}, C^d\}}{1+|m|+|n|}\right)\right)^2.$$

Collecting terms together, and then upper bounding $\min\{\mathcal{X}/C^d, \mathcal{X}/|n|\}^{q(q-1)}$ by $(\mathcal{X}/(1+|n|))^{q(q-1)}$ and upper bounding $\min\{\mathcal{X}, C^d\}$ everywhere else by C^d, the above is

$$\ll \left(\frac{\mathcal{X}}{1+|n|}\right)^{q(q-1)} \sum_{(r-1)D<d\leq rD} \frac{C^{O(1)}}{C^{2(2-q)d}} \mathcal{X}^{q^2} C^{(3-q^2)d} = \left(\frac{\mathcal{X}}{1+|n|}\right)^{q(q-1)} C^{O(1)} \mathcal{X}^{q^2} C^{-(q-1)^2(r-1)D}.$$

We can also adapt the Steinhaus argument to bound $\mathbb{E} \max_{(r-1)D<d\leq rD} G_d(n)^q H_d(n) C^{2(q-1)d}$. In this case we again have $\mathbb{E}\big|F_k\big(\frac{1}{2}+\sigma+i\big(\frac{n}{\mathcal{X}}+t\big)\big)\big|^2 \asymp \mathcal{X}$, and we may define the "tilted" measure $\tilde{\mathbb{P}}$ and set $L_d := \prod_{p\leq e^{\mathcal{X}/C^d}} |1+f(p)/p^{1/2+\sigma+i(n/\mathcal{X}+t)}|^{2(q-1)/1.01}$ analogously to the Steinhaus case. Then Euler Product Result 2.2 implies that $\tilde{\mathbb{E}} L_d \asymp \min\{\mathcal{X}/C^d, \mathcal{X}/|n|\}^{(1+(q-1)/1.01)(q-1)/1.01}(1+\mathcal{X}/C^d)^{2(q-1)/1.01+(q-1)^2/1.01^2}$ and $\tilde{\mathbb{E}} L_d^{1.01} \asymp \min\{\mathcal{X}/C^d, \mathcal{X}/|n|\}^{q(q-1)}(1+\mathcal{X}/C^d)^{2(q-1)+(q-1)^2}$. So the same submartingale argument as in the Steinhaus case shows that

$$\mathbb{E} \max_{(r-1)D<d\leq rD} G_d(n)^q H_d(n) C^{2(q-1)d} \ll \mathcal{X}^{1+2(q-1)} \left(1+\frac{\mathcal{X}}{C^{(r-1)D+1}}\right)^{(q-1)^2} \min\left\{\frac{\mathcal{X}}{C^{(r-1)D+1}}, \frac{\mathcal{X}}{|n|}\right\}^{q(q-1)}$$
$$\ll \frac{\mathcal{X}^{q^2}}{C^{(r-1)D(q-1)^2}} \left(\frac{\mathcal{X}}{1+|n|}\right)^{q(q-1)}.$$

Putting everything together, recalling that $C = e^{1/(q-1)}$ and choosing $D := \lfloor 1/(q-1) \rfloor$, we deduce that (5-6) is

$$\ll D^{q-1} \sum_{|n|\leq \frac{\mathcal{X}}{2}+1} \sum_{r\leq \frac{(q-1)\log \mathcal{X}}{D}+1} \frac{\mathcal{X}^{q^2}}{C^{(r-1)D(q-1)^2}} \left(\frac{\mathcal{X}}{1+|n|}\right)^{q(q-1)} \ll \mathcal{X}^{q^2} \sum_{|n|\leq \frac{\mathcal{X}}{2}+1} \left(\frac{\mathcal{X}}{1+|n|}\right)^{q(q-1)}.$$

Since $q_0 = (1+\sqrt{5})/2 \approx 1.618$ satisfies $q_0(q_0-1) = 1$, and we have $1 < q < 2$, the sum over n here is $\ll \mathcal{X}^{\max\{1, q(q-1)\}} \min\{\log \mathcal{X}, 1/|q-q_0|\}$. Substituting into (5-2), and recalling that $\mathcal{X} := \min\{\log x/e^{k+1}, 1/|\sigma|\}$, this gives the first $(N=0)$ bound claimed in Key Proposition 5.2 when $1 < q < 2$.

□

6. Proofs of the lower bounds in Theorems 1.1 and 1.2

Recall that $F(s)$ denotes the Euler product of $f(n)$ over x-smooth numbers.

The lower bound in the Steinhaus case. To prove the lower bound part of Theorem 1.1, in view of Proposition 4.3 our main work will be to prove a suitable lower bound for $\| \int_{-1/2}^{1/2} |F(\frac{1}{2}+\frac{4Vq}{\log x}+it)|^2 \, dt \|_q$, where V is a large fixed constant. (We also need an upper bound for the subtracted quantity $\| \int_{-1/2}^{1/2} |F(\frac{1}{2}+\frac{2Vq}{\log x}+it)|^2 \, dt \|_q$, but this will follow directly from Key Proposition 5.1.)

To obtain our lower bound, we note first that for any $q \geq 1$ we have

$$\left(\int_{-1/2}^{1/2} \left| F\left(\frac{1}{2}+\frac{4Vq}{\log x}+it\right)\right|^2 dt \right)^q \geq \left(\sum_{|k| \leq (\log x - 1)/2} \int_{(k-1/2)/\log x}^{(k+1/2)/\log x} \left| F\left(\frac{1}{2}+\frac{4Vq}{\log x}+it\right)\right|^2 dt \right)^q$$
$$\geq \sum_{|k| \leq (\log x - 1)/2} \left(\int_{(k-1/2)/\log x}^{(k+1/2)/\log x} \left| F\left(\frac{1}{2}+\frac{4Vq}{\log x}+it\right)\right|^2 dt \right)^q .$$

This step could be wasteful if many of the pieces $\int_{(k-1/2)/\log x}^{(k+1/2)/\log x} |F(\frac{1}{2}+\frac{4Vq}{\log x}+it)|^2 \, dt$ made substantial contributions to the full integral. But for large q we expect instead that the dominant contribution should come from just a few large (and therefore rare) contributions, so we will not lose too much. In the Steinhaus case, since the distribution of $\int_{(k-1/2)/\log x}^{(k+1/2)/\log x} |F(\frac{1}{2}+\frac{4Vq}{\log x}+it)|^2 \, dt$ is independent of k we get the simpler lower bound

$$\mathbb{E}\left(\int_{-1/2}^{1/2} \left| F\left(\frac{1}{2}+\frac{4Vq}{\log x}+it\right)\right|^2 dt \right)^q \gg \log x \cdot \mathbb{E}\left(\int_{-1/(2\log x)}^{1/(2\log x)} \left| F\left(\frac{1}{2}+\frac{4Vq}{\log x}+it\right)\right|^2 dt \right)^q .$$

Now we want to remove the remaining short integral over t, which is a technical obstacle to connecting up the expectation with the random product F. Heuristically, since the Euler product shouldn't vary much on intervals of length $1/\log x$ we should simply obtain something like $(\frac{1}{\log x} |F(\frac{1}{2}+\frac{4Vq}{\log x})|^2)^q$ in the bracket. It turns out that a neat way to handle this issue is using Jensen's inequality (applied to the normalized integral $\int_{-1/2\log x}^{1/2\log x} \log x \, dt$), which implies that

$$\mathbb{E}\left(\int_{-1/(2\log x)}^{1/(2\log x)} \left| F\left(\frac{1}{2}+\frac{4Vq}{\log x}+it\right)\right|^2 dt \right)^q$$
$$= \frac{1}{\log^q x} \mathbb{E}\left(\int_{-1/(2\log x)}^{1/(2\log x)} \log x \cdot e^{2\log |F(1/2+4Vq/\log x + it)|} \, dt \right)^q$$
$$\geq \frac{1}{\log^q x} \mathbb{E}\left(\exp\left\{ \int_{-1/(2\log x)}^{1/(2\log x)} \log x \cdot 2 \log \left| F\left(\frac{1}{2}+\frac{4Vq}{\log x}+it\right)\right| dt \right\} \right)^q$$
$$= \frac{1}{\log^q x} \mathbb{E} \exp\left\{ 2q \int_{-1/(2\log x)}^{1/(2\log x)} \log x \cdot \log \left| F\left(\frac{1}{2}+\frac{4Vq}{\log x}+it\right)\right| dt \right\}.$$

Here the exponential, inside the expectation, may be rewritten as

$$\prod_{p\le x}\exp\left\{-2q\int_{-1/(2\log x)}^{1/(2\log x)}\log x\cdot\Re\log\left(1-\frac{f(p)}{p^{1/2+4Vq/\log x+it}}\right)dt\right\}$$
$$=\prod_{p\le x}\exp\left\{2q\log x\,\Re\left(\frac{f(p)}{p^{1/2+4Vq/\log x}}\int_{-1/(2\log x)}^{1/(2\log x)}e^{-it\log p}\,dt\right.\right.$$
$$\left.\left.+\frac{f(p)^2}{2p^{1+8Vq/\log x}}\int_{-1/(2\log x)}^{1/(2\log x)}e^{-2it\log p}\,dt\right)+O\left(\frac{q}{p^{3/2}}\right)\right\}$$
$$=e^{O(q)}\prod_{p\le x}\exp\left\{2q\Re\left(\frac{f(p)}{p^{1/2+4Vq/\log x}}\log x\int_{-1/(2\log x)}^{1/(2\log x)}e^{-it\log p}\,dt+\frac{f(p)^2}{2p^{1+8Vq/\log x}}\right)\right\}.$$

The first equality here uses the Taylor expansion of the logarithm, and the second equality uses the estimate

$$\int_{-1/(2\log x)}^{1/(2\log x)}e^{-2it\log p}\,dt=\int_{-1/(2\log x)}^{1/(2\log x)}(1+O(|t|\log p))\,dt=\frac{1}{\log x}+O\left(\frac{\log p}{\log^2 x}\right)$$

and also the fact that

$$\sum_{p\le x}\frac{\log p}{p^{1+8Vq/\log x}}\ll\log x.$$

Putting things together, using the independence of $f(p)$ for different primes p to move the expectation inside the product, we have shown that our original object

$$\mathbb{E}\left(\int_{-1/2}^{1/2}\left|F\left(\frac{1}{2}+\frac{4Vq}{\log x}+it\right)\right|^2dt\right)^q$$
$$\ge\frac{e^{O(q)}}{\log^{q-1}x}\prod_{p\le x}\mathbb{E}\exp\left\{2q\Re\left(\frac{f(p)}{p^{1/2+4Vq/\log x}}\log x\int_{-1/(2\log x)}^{1/(2\log x)}e^{-it\log p}\,dt+\frac{f(p)^2}{2p^{1+8Vq/\log x}}\right)\right\}.\quad(6\text{-}1)$$

It will be convenient to note some simple bounds for the quantity inside the exponential, which we will use shortly. Firstly, this quantity is always trivially bounded by $O(q/\sqrt{p})$. Secondly, using our previous calculation that

$$\int_{-1/(2\log x)}^{1/(2\log x)}e^{-it\log p}\,dt=\frac{1}{\log x}+O\left(\frac{\log p}{\log^2 x}\right),$$

we can obtain that

$$2q\Re\left(\frac{f(p)}{p^{1/2+4Vq/\log x}}\log x\int_{-1/(2\log x)}^{1/(2\log x)}e^{-it\log p}\,dt+\frac{f(p)^2}{2p^{1+8Vq/\log x}}\right)$$
$$=\frac{2q\Re f(p)}{p^{1/2+4Vq/\log x}}+O\left(\frac{q\log p}{p^{1/2+4Vq/\log x}\log x}+\frac{q}{p}\right).$$

To conclude, we note that certainly when $100q^2 \le p \le x$ we have, in view of the Taylor expansion of the exponential and the simple bounds noted above and the fact that $\mathbb{E}(\Re f(p))^2 = \frac{1}{2}$, that

$$\begin{aligned}
&\mathbb{E}\exp\biggl\{2q\Re\biggl(\frac{f(p)}{p^{1/2+4Vq/\log x}}\log x\int_{-1/(2\log x)}^{1/(2\log x)} e^{-it\log p}\,dt+\frac{f(p)^2}{2p^{1+8Vq/\log x}}\biggr)\biggr\} \\
&\quad=\mathbb{E}\biggl(1+2q\Re\biggl(\frac{f(p)}{p^{1/2+4Vq/\log x}}\log x\int_{-1/(2\log x)}^{1/(2\log x)} e^{-it\log p}\,dt+\frac{f(p)^2}{2p^{1+8Vq/\log x}}\biggr)+\frac{2q^2(\Re f(p))^2}{p^{1+8Vq/\log x}} \\
&\qquad\qquad+O\biggl(\frac{q^2\log p}{p^{1+8Vq/\log x}\log x}+\frac{q^3}{p^{3/2}}\biggr)\biggr) \\
&\quad=1+\frac{q^2}{p^{1+8Vq/\log x}}+O\biggl(\frac{q^2\log p}{p^{1+8Vq/\log x}\log x}+\frac{q^3}{p^{3/2}}\biggr).
\end{aligned}$$

When $p < 100q^2$, we shall instead use the trivial bound $\exp\{O(q/\sqrt{p})\}$. Inserting these into (6-1), we get an overall lower bound

$$\begin{aligned}
&\mathbb{E}\biggl(\int_{-1/2}^{1/2}\bigl|F\bigl(\tfrac{1}{2}+\tfrac{4Vq}{\log x}+it\bigr)\bigr|^2\,dt\biggr)^q \\
&\quad\ge\frac{e^{O(q)}}{\log^{q-1}x}\prod_{p<100q^2}\exp\biggl\{O\biggl(\frac{q}{\sqrt{p}}\biggr)\biggr\}\prod_{100q^2\le p\le x}\exp\biggl\{\frac{q^2}{p^{1+8Vq/\log x}}+O\biggl(\frac{q^2\log p}{p^{1+8Vq/\log x}\log x}+\frac{q^3}{p^{3/2}}\biggr)\biggr\} \\
&\quad=\frac{e^{O(q^2/\log(2q))}}{\log^{q-1}x}\prod_{100q^2\le p\le x}\exp\biggl\{\frac{q^2}{p^{1+8Vq/\log x}}\biggr\} \\
&\quad=\frac{e^{O(q^2)}}{\log^{q-1}x}\biggl(\frac{\log x}{Vq\log(2q)}\biggr)^{q^2}.
\end{aligned}$$

Here the final equality follows because, similarly as in the calculations in Section 3, we have

$$\prod_{100q^2\le p\le x}\exp\biggl\{\frac{q^2}{p^{1+8Vq/\log x}}\biggr\}=e^{O(q^2)}\zeta\biggl(1+\frac{8Vq}{\log x}\biggr)^{q^2}e^{-\sum_{p<100q^2}\frac{q^2}{p^{1+8Vq/\log x}}}.$$

Then

$$\zeta\biggl(1+\frac{8Vq}{\log x}\biggr)^{q^2}=e^{O(q^2)}\biggl(\frac{\log x}{Vq}\biggr)^{q^2}\quad\text{and}\quad e^{-\sum_{p<100q^2}\frac{q^2}{p^{1+8Vq/\log x}}}=\frac{e^{O(q^2)}}{\log^{q^2}(2q)}$$

by Mertens' estimates for sums over primes.

Inserting this into Proposition 4.3 we find that

$$\Bigl\|\sum_{n\le x}f(n)\Bigr\|_{2q}\gg\sqrt{\frac{x}{\log x}}\biggl(\frac{e^{O(q)}}{\log^{(q-1)/2q}x}\biggl(\frac{\log x}{Vq\log(2q)}\biggr)^{q/2}-\frac{C}{e^{Vq/2}}\biggl\|\int_{-1/2}^{1/2}\biggl|F\biggl(\frac{1}{2}+\frac{2Vq}{\log x}+it\biggr)\biggr|^2\,dt\biggr\|_q^{1/2}\biggr).$$

And using Key Proposition 5.1 with $k=-1$ to control the subtracted term, provided that $2Vq/\log x \le 1/(100\log(2q))$ we can bound everything below by

$$\sqrt{\frac{x}{\log x}}\left(\frac{e^{O(q)}}{\log^{(q-1)/2q} x}\left(\frac{\log x}{Vq\log(2q)}\right)^{q/2} - \frac{Ce^{O(q)}}{e^{Vq/2}}\frac{(Vq)^{(q-1)/2q}}{\log^{(q-1)/2q} x}\left(\frac{\log x}{Vq\log(2q)}\right)^{q/2}\right).$$

If we set V to be a sufficiently large fixed constant, the subtracted term will be negligible compared with the first term, and our Theorem 1.1 lower bound will be proved. It only remains to note that the condition $2Vq/\log x \leq 1/(100\log(2q))$ is then satisfied provided $q \leq (c\log x)/\log\log x$, for a sufficiently small fixed constant $c > 0$. □

The lower bound in the Rademacher case. To prove the lower bound part of Theorem 1.2, we shall invoke Proposition 4.4 and adapt the argument from the previous subsection to lower bound $\| \int_{-1/2}^{1/2} |F(\frac{1}{2}+\frac{4Vq}{\log x}+it)|^2\, dt\|_q$, where V is a large fixed constant and now $F(s)$ denotes the Rademacher random Euler product.

Indeed, exactly the same argument as on page 2315 gives, for any $q \geq 1$, that

$$\mathbb{E}\left(\int_{-1/2}^{1/2} |F(\tfrac{1}{2}+\tfrac{4Vq}{\log x}+it)|^2\, dt\right)^q \geq \sum_{|k|\leq(\log x-1)/2} \mathbb{E}\left(\int_{(k-1/2)/\log x}^{(k+1/2)/\log x} |F(\tfrac{1}{2}+\tfrac{4Vq}{\log x}+it)|^2\, dt\right)^q.$$

Using Jensen's inequality, also as on page 2315, shows this is all

$$\geq \frac{1}{\log^q x}\sum_{|k|\leq(\log x-1)/2} \mathbb{E}\exp\left\{2q\int_{(k-1/2)/\log x}^{(k+1/2)/\log x} \log x\cdot\log|F(\tfrac{1}{2}+\tfrac{4Vq}{\log x}+it)|\, dt\right\}.$$

And recalling that in the Rademacher case we have $F(s)=\prod_{p\leq x}(1+f(p)/p^s)$, with $f(p)\in\{\pm1\}$, we find this is all

$$= \frac{1}{\log^q x}\sum_{|k|\leq(\log x-1)/2}\prod_{p\leq x}\mathbb{E}\exp\left\{2q\int_{(k-1/2)/\log x}^{(k+1/2)/\log x}\log x\cdot\Re\log\left(1+\frac{f(p)}{p^{1/2+4Vq/\log x+it}}\right)dt\right\}$$

$$= \frac{1}{\log^q x}\sum_{|k|\leq(\log x-1)/2}\prod_{p\leq x}\mathbb{E}\exp\left\{2q\int_{(k-1/2)/\log x}^{(k+1/2)/\log x}\log x\cdot\left(\frac{f(p)\cos(t\log p)}{p^{1/2+4Vq/\log x}} - \frac{\cos(2t\log p)}{2p^{1+8Vq/\log x}} + O\left(\frac{1}{p^{3/2}}\right)\right)dt\right\}.$$

At this stage we cannot efficiently remove the integral of $\cos(t\log p)$ in the first term, but for the second term we can write $\cos(2t\log p)=\cos(2k\log p/\log x)+O(\log p/\log x)$. The total contribution from these "big Oh" terms for all p, as well as from the $O(1/p^{3/2})$ term, is a multiplicative factor $e^{O(q)}$. So we obtain that

$$\mathbb{E}\left(\int_{-1/2}^{1/2}|F(\tfrac{1}{2}+\tfrac{4Vq}{\log x}+it)|^2\, dt\right)^q \geq \frac{e^{O(q)}}{\log^q x}\sum_{|k|\leq(\log x-1)/2}\prod_{p\leq x}\mathbb{E}\exp\left\{2q\left(\frac{f(p)}{p^{1/2+4Vq/\log x}}\log x\int_{(k-1/2)/\log x}^{(k+1/2)/\log x}\cos(t\log p)\, dt - \frac{\cos(2k\log p/\log x)}{2p^{1+8Vq/\log x}}\right)\right\}, \quad (6\text{-}2)$$

which is the Rademacher analogue of (6-1) from the Steinhaus case.

Next, when $100q^2 \le p \le x$ we have, in view of the Taylor expansion of the exponential (and the fact that $f(p)^2 \equiv 1$), that

$$\mathbb{E}\exp\left\{2q\left(\frac{f(p)}{p^{1/2+4Vq/\log x}}\log x\int_{(k-1/2)/\log x}^{(k+1/2)/\log x}\cos(t\log p)\,dt-\frac{\cos(2k\log p/\log x)}{2p^{1+8Vq/\log x}}\right)\right\}$$
$$=\mathbb{E}\left(1+2q\left(\frac{f(p)}{p^{1/2+4Vq/\log x}}\log x\int_{(k-1/2)/\log x}^{(k+1/2)/\log x}\cos(t\log p)\,dt-\frac{\cos(2k\log p/\log x)}{2p^{1+8Vq/\log x}}\right)\right.$$
$$\left.+\frac{2q^2\cos^2(k\log p/\log x)}{p^{1+8Vq/\log x}}+O\left(\frac{q^2\log p}{p^{1+8Vq/\log x}\log x}+\frac{q^3}{p^{3/2}}\right)\right).$$

Using the cosine identity $\cos^2(k\log p/\log x)=\left(\frac{1}{2}\right)(1+\cos(2k\log p/\log x))$, and the fact that $\mathbb{E}f(p)=0$, we find the above is

$$=1+\frac{q^2+(q^2-q)\cos(2k\log p/\log x)}{p^{1+8Vq/\log x}}+O\left(\frac{q^2\log p}{p^{1+8Vq/\log x}\log x}+\frac{q^3}{p^{3/2}}\right).$$

When $p<100q^2$, we shall instead use the trivial bound $\exp\{O(q/\sqrt{p})\}$. Inserting these into (6-2), we get

$$\mathbb{E}\left(\int_{-1/2}^{1/2}\left|F\left(\tfrac{1}{2}+\tfrac{4Vq}{\log x}+it\right)\right|^2dt\right)^q$$
$$\ge\frac{e^{O(q^2/\log(2q))}}{\log^q x}\sum_{|k|\le(\log x-1)/2}\prod_{100q^2\le p\le x}\exp\left\{\frac{q^2+(q^2-q)\cos(2k\log p/\log x)}{p^{1+8Vq/\log x}}\right\}.$$

Now when $2\le q\le c\log x/\log\log x$, say, we can afford to discard all the terms in this lower bound except the $k=0$ term, which gives us that

$$\mathbb{E}\left(\int_{-1/2}^{1/2}\left|F\left(\tfrac{1}{2}+\tfrac{4Vq}{\log x}+it\right)\right|^2dt\right)^q\ge\frac{e^{O(q^2/\log(2q))}}{\log^q x}\prod_{100q^2\le p\le x}\exp\left\{\frac{2q^2-q}{p^{1+8Vq/\log x}}\right\}$$
$$=\frac{e^{O(q^2)}}{\log^q x}\left(\frac{\log x}{Vq\log(2q)}\right)^{2q^2-q}.$$

Inserting this into Proposition 4.4, and applying Key Proposition 5.2 with $k=-1$ and $\sigma=2Vq/\log x$ to control the subtracted term there, we find that $\left\|\sum_{n\le x}f(n)\right\|_{2q}$ is

$$\gg\sqrt{\frac{x}{\log x}}\left(\frac{e^{O(q)}}{\log^{1/2}x}\left(\frac{\log x}{Vq\log(2q)}\right)^{q-1/2}-\frac{Ce^{O(q)}}{e^{Vq/2}}\frac{(Vq)^{1/2}}{\log^{1/2}x}\left(\frac{\log x}{Vq\log(2q)}\right)^{q-1/2}\right).$$

If V is a sufficiently large constant, the subtracted term is negligible compared with the first term and we obtain the lower bound claimed in Theorem 1.2.

When $1\le q<2$ (or really when $1\le q\le q_0=(1+\sqrt{5})/2$), we cannot afford to take quite such a crude approach. Using Chebychev's estimates and the prime number theorem as in the proof of Euler Product

Result 2.1, we have

$$\sum_{100q^2\le p\le x} \frac{\cos(2k\log p/\log x)}{p^{1+8Vq/\log x}} = \sum_{2\le p\le x^{1/V}} \frac{\cos(2k\log p/\log x)}{p} + O(1)$$
$$= \int_{\log 2}^{\log(x^{1/V})} \frac{\cos((2k/\log x)u)}{u}\,du + O(1)$$
$$= \log\min\{\log(x^{1/V}), \log(x^{1/(1+|k|)})\} + O(1).$$

Using this estimate, we get a lower bound for $\mathbb{E}\big(\int_{-1/2}^{1/2}\big|F\big(\frac{1}{2}+\frac{4Vq}{\log x}+it\big)\big|^2\,dt\big)^q$ that is

$$\gg \frac{1}{\log^q x}\left(\frac{\log x}{V}\right)^{q^2} \sum_{|k|\le(\log x-1)/2} \min\left\{\frac{\log x}{V}, \frac{\log x}{1+|k|}\right\}^{q^2-q},$$

and (remembering that q_0 satisfies $q_0^2 - q_0 = 1$) this is

$$\gg \frac{1}{\log^q x}\left(\frac{\log x}{V}\right)^{q^2+\max\{1,q^2-q\}} \min\left\{\log\log x, \frac{1}{|q-q_0|}\right\}.$$

Again, inserting this in Proposition 4.4 produces the lower bound claimed in Theorem 1.2. □

Acknowledgements

The author would like to thank the anonymous referee, for helpful comments and suggestions.

References

[Bonami 1970] A. Bonami, "Étude des coefficients de Fourier des fonctions de $L^p(G)$", *Ann. Inst. Fourier (Grenoble)* **20**:2 (1970), 335–402. MR Zbl

[Bondarenko et al. 2018] A. Bondarenko, O. F. Brevig, E. Saksman, K. Seip, and J. Zhao, "Pseudomoments of the Riemann zeta function", *Bull. Lond. Math. Soc.* **50**:4 (2018), 709–724. MR Zbl

[Chandee 2011] V. Chandee, "On the correlation of shifted values of the Riemann zeta function", *Q. J. Math.* **62**:3 (2011), 545–572. MR Zbl

[Florea 2017] A. Florea, "The fourth moment of quadratic Dirichlet L-functions over function fields", *Geom. Funct. Anal.* **27**:3 (2017), 541–595. MR Zbl

[Granville and Soundararajan 2001] A. Granville and K. Soundararajan, "Large character sums", *J. Amer. Math. Soc.* **14**:2 (2001), 365–397. MR Zbl

[Gut 2013] A. Gut, *Probability: a graduate course*, 2nd ed., Springer, 2013. MR Zbl

[Halász 1983] G. Halász, "On random multiplicative functions", pp. 74–96 in *Hubert Delange colloquium* (Orsay, France, 1982), Publ. Math. Orsay **83**, Univ. Paris XI, 1983. MR Zbl

[Harper 2017] A. J. Harper, "Moments of random multiplicative functions, I: Low moments, better than squareroot cancellation, and critical multiplicative chaos", preprint, 2017. To appear in *Forum of Mathematics, Pi*. arXiv

[Harper et al. 2015] A. J. Harper, A. Nikeghbali, and M. Radziwiłł, "A note on Helson's conjecture on moments of random multiplicative functions", pp. 145–169 in *Analytic number theory*, edited by C. Pomerance and M. T. Rassias, Springer, 2015. MR Zbl

[Heap and Lindqvist 2016] W. P. Heap and S. Lindqvist, "Moments of random multiplicative functions and truncated characteristic polynomials", *Q. J. Math.* **67**:4 (2016), 683–714. MR Zbl

[Helson 2010] H. Helson, "Hankel forms", *Studia Math.* **198**:1 (2010), 79–84. MR Zbl

[Ivić 2003] A. Ivić, *The Riemann zeta-function: Theory and applications*, Dover, Mineola, NY, 2003. Zbl

[Keating and Odgers 2008] J. P. Keating and B. E. Odgers, "Symmetry transitions in random matrix theory and L-functions", *Comm. Math. Phys.* **281**:2 (2008), 499–528. MR Zbl

[Lau et al. 2013] Y.-K. Lau, G. Tenenbaum, and J. Wu, "On mean values of random multiplicative functions", *Proc. Amer. Math. Soc.* **141**:2 (2013), 409–420. MR Zbl

[Montgomery and Vaughan 2007] H. L. Montgomery and R. C. Vaughan, *Multiplicative number theory, I: Classical theory*, Cambridge Stud. Adv. Math. **97**, Cambridge Univ. Press, 2007. MR Zbl

[Munsch 2017] M. Munsch, "Shifted moments of L-functions and moments of theta functions", *Mathematika* **63**:1 (2017), 196–212. MR Zbl

[Munsch and Shparlinski 2016] M. Munsch and I. E. Shparlinski, "Upper and lower bounds for higher moments of theta functions", *Q. J. Math.* **67**:1 (2016), 53–73. MR Zbl

[Saksman and Seip 2016] E. Saksman and K. Seip, "Some open questions in analysis for Dirichlet series", pp. 179–191 in *Recent progress on operator theory and approximation in spaces of analytic functions*, edited by C. Bénéteau et al., Contemp. Math. **679**, Amer. Math. Soc., Providence, RI, 2016. MR Zbl

[Shi and Weber 2016] S. Y. Shi and M. Weber, "On the equation $n_1 \cdots n_{k+1} = n_{k+2} \cdots n_{2(k+1)}$ and some variant with restricted unknowns", preprint, 2016. arXiv

[Soundararajan and Young 2010] K. Soundararajan and M. P. Young, "The second moment of quadratic twists of modular L-functions", *J. Eur. Math. Soc.* **12**:5 (2010), 1097–1116. MR Zbl

[Wintner 1944] A. Wintner, "Random factorizations and Riemann's hypothesis", *Duke Math. J.* **11** (1944), 267–275. MR Zbl

Communicated by Roger Heath-Brown
Received 2018-04-27 Revised 2019-04-24 Accepted 2019-07-05

a.harper@warwick.ac.uk *University of Warwick, Coventry, United Kingdom*

ALGEBRA AND NUMBER THEORY 13:10 (2019)
dx.doi.org/10.2140/ant.2019.13.2323

Artin–Mazur–Milne duality for fppf cohomology

Cyril Demarche and David Harari

We provide a complete proof of a duality theorem for the fppf cohomology of either a curve over a finite field or a ring of integers of a number field, which extends the classical Artin–Verdier Theorem in étale cohomology. We also prove some finiteness and vanishing statements.

1. Introduction

Let K be a number field or the function field of a smooth, projective, geometrically integral curve X over a finite field. In the number field case, set $X := \operatorname{Spec} \mathcal{O}_K$, where $\mathcal{O}_K$ is the ring of integers of K. Let U be a nonempty Zariski open subset of X and denote by N a commutative, finite and flat group scheme over U with Cartier dual N^D. Assume that the order of N is invertible on U (in particular N is étale). The classical "étale" *Artin–Verdier Theorem* [Milne 1986, Corollary II.3.3] is a duality statement between étale cohomology $H^\bullet_{\text{ét}}(U, N)$ and étale cohomology with compact support $H^\bullet_{\text{ét},c}(U, N^D)$. It has been known for a long time that this theorem is especially useful in view of concrete arithmetic applications: for example it yields a very nice method to prove deep results like Cassels–Tate duality for abelian varieties and schemes [Milne 1986, Section II.5] and their generalizations to 1-motives [Harari and Szamuely 2005, Section 4]; Artin–Verdier's Theorem also provides a "canonical" path to prove the Poitou–Tate's Theorem and its extension to complex of tori [Demarche 2011b], which in turn turns out to be very fruitful to deal with local-global questions for (not necessarily commutative) linear algebraic groups [Demarche 2011a].

It is of course natural to try to remove the condition that the order of N is invertible on U. A good framework to do this is provided by fppf cohomology of finite and flat commutative group schemes over U, as introduced by J.S. Milne in the third part of his book [1986]. This includes the case of group schemes of order divisible by $p := \operatorname{Char} K$ in the function field case.

Such an fppf duality theorem was first announced by B. Mazur [1972, Proposition 7.2],[1] relying on work by M. Artin and himself. Special cases have also been proved by M. Artin and Milne [1976]. The precise statement of the theorem is as follows (see [Milne 1986], Corollary III.3.2 for the number field case and Theorem III.8.2 for the function field case):

MSC2010: primary 11G20; secondary 14H25.
Keywords: fppf cohomology, arithmetic duality, Artin approximation theorem.

[1] Thanks to A. Schmidt for having pointed this out to us.

Theorem 1.1. *Let $j : U \hookrightarrow X$ be a nonempty open subscheme of X. Let N be a finite flat commutative group scheme over U with Cartier dual N^D. For all integers r with $0 \leq r \leq 3$, the canonical pairing*

$$H_c^{3-r}(U, N) \times H^r(U, N^D) \to H_c^3(U, \boldsymbol{G}_m) \cong \mathbb{Q}/\mathbb{Z}$$

(*where $H^r(U, N^D)$ is an fppf cohomology group and $H_c^{3-r}(U, N)$ an fppf cohomology group with compact support*) *induces a perfect duality between the profinite group $H_c^{3-r}(U, N)$ and the discrete group $H^r(U, N^D)$. Besides, these groups are finite in the number field case, and they are trivial for $r \geq 4$ and $r < 0$* (*resp. for $r = 3$ if $U \neq X$*) *in the function field case.*

For example, this extension of the étale Artin–Verdier Theorem is needed to prove the Poitou–Tate exact sequence over global fields of characteristic p [González-Avilés 2009, Theorems 4.8 and 4.11] as well as the Poitou–Tate Theorem over a global field without restriction on the order ([Česnavičius 2015a, Theorem 5.1], which in turn is used in [Rosengarten 2018, Sections 5.6 and 5.7]). Results of [Milne 1986, Section III.9] (which rely on the fppf duality Theorem) are also a key ingredient in the proof of some cases of the Birch and Swinnerton-Dyer conjecture for abelian varieties over global fields of positive characteristic, in [Bauer 1992, Section 4] and [Kato and Trihan 2003, Section 2] for instance. Our initial interest in Theorem 1.1 was to try to extend it to complexes of tori in the function field case, following the same method as in the number field case [Demarche 2011b]. Such a generalization should then provide results (known in the number field case) about weak and strong approximation for linear algebraic groups defined over a global field of positive characteristic.

However, as K. Česnavičius pointed out to us,[2] it seems necessary to add details to the proof in [Milne 1986], Sections III.3. and III.8, for two reasons:

- The functoriality of flat cohomology with compact support and the commutativity of several diagrams are not explained in [Milne 1986]. Even in the case of an imaginary number field, a definition of $H_c^r(U, \mathcal{F})$ as $H^r(X, j_! \mathcal{F})$ for an fppf sheaf $\mathcal{F}$ (which works for the étale Artin–Verdier Theorem) would not be the right one, because it does not provide the key exact sequence [loc. cit., Proposition III.0.4.a] in the fppf setting: indeed the proof of this exact sequence relies on [loc. cit., Lemma II.2.4], which in turn uses [loc. cit., Proposition II.1.1]; but the analogue of the latter does not stand anymore with étale cohomology replaced by fppf cohomology, see also Remark 2.2 of the present paper.

It is therefore necessary to work with an ad hoc definition of compact support cohomology as in [loc. cit., Section III.0]. Since this definition involves mapping cones, commutativities of some diagrams have to be checked in the category of complexes and not in the derived category (where there is no good functoriality for the mapping cones). Typically, the isomorphisms that compute $C^\bullet(b)$, $C^\bullet(b \circ a)$ and $C^\bullet(c \circ b \circ a)$ in [loc. cit., Proposition III.0.4.c] are not canonical a priori. Hence the required compatibilities in [loc. cit., proof of Theorem III.3.1. and Lemma III.8.4] have to be checked carefully.

[2] In particular, he observed that the analogue of [Milne 1986, Proposition III.0.4.c] is by no means obvious when henselizations are replaced by completions. This analogue is actually false without additional assumptions, as shown by T. Suzuki [2018, Remark 2.7.9]

• In the positive characteristic case, it is necessary (as explained in [Milne 1986, Section III.8]) to work with a definition of cohomology with compact support involving *completions* of the local rings of points in $X \setminus U$ instead of their henselizations. The reason is that a local duality statement [loc. cit., Theorem III.6.10] is needed and this one only works in the context of complete valuation fields, in particular because the H^1 groups involved have to be locally compact (so that Pontryagin duality makes sense). It turns out that some properties of compact support cohomology (in particular [loc. cit., Proposition III.0.4.c]) are more difficult to establish in this context: for example the comparison between cohomology of the completion $\hat{\mathcal{O}}_v$ and of the henselization $\mathcal{O}_v$ is not as straightforward as in the étale case.

The goal of this article is to present a detailed proof of Theorem 1.1 with special regards to the two issues listed above. Section 2 is devoted to general properties of fppf cohomology with compact support (Proposition 2.1), which involves some homological algebra (Lemma 2.3) as well as comparison statements between cohomology of $\mathcal{O}_v$ and $\hat{\mathcal{O}}_v$ (Lemma 2.6); besides, we make the link to classical étale cohomology with compact support (Lemma 2.10).

We also define a natural topology on the fppf compact support cohomology groups (see Section 3) and prove its basic properties. In Section 4, we follow the method of [Milne 1986, Section III.8] to prove Theorem 1.1 in the function field case. As a corollary, we get a finiteness statement (Corollary 4.9), which apparently has not been observed before this paper. The case of a number field is simpler once the functorial properties of Section 2 have been proved; it is treated in Section 5. Finally, we include two useful results in homological algebra in the Appendix.

One week after the first draft of this article was released, Takashi Suzuki kindly informed us that in his preprint [Suzuki 2018], he obtained (essentially at the same time as us) fppf duality results similar to Theorem 1.1 in a slightly more general context.[3] His methods are somehow more involved than ours, they use the *rational étale site*, which he developed in earlier papers.

Notation. Let X be either a smooth projective curve over a finite field k of characteristic p, or the spectrum of the ring of integers $\mathcal{O}_K$ of a number field K. Let $K := k(X)$ be the function field of X. Throughout the paper, schemes S are endowed with a big fppf site $(\mathrm{Sch}/S)_{\mathrm{fppf}}$ in the sense of [Stacks 2005–, Tag 021R, Tag 021S, Tag 03XB]. By construction, the underlying category in $(\mathrm{Sch}/S)_{\mathrm{fppf}}$ is small and the family of coverings for this site is a set. The corresponding topos is independent of the choices made thanks to [Stacks 2005–, Tag 00VY]. In contrast with [SGA 4_1 1972], the construction of the site $(\mathrm{Sch}/S)_{\mathrm{fppf}}$ in [Stacks 2005–] does not require the existence of universes. The reader who is ready to accept this axiom can replace the site $(\mathrm{Sch}/S)_{\mathrm{fppf}}$ by the big fppf site from [SGA 4_1 1972].

Unless stated otherwise, cohomology is fppf cohomology with respect to this site.

For any closed point $v \in X$, let $\mathcal{O}_v$ (resp. $\hat{\mathcal{O}}_v$) be the henselization (resp. the completion) of the local ring $\mathcal{O}_{X,v}$ of X at v. Let K_v (resp. $\hat{K}_v$) be the fraction field of $\mathcal{O}_v$ (resp. $\hat{\mathcal{O}}_v$). Let U be a nonempty Zariski open subset of X and denote by $j : U \to X$ the corresponding open immersion. By [Matsumura 1970, Section 34],

[3] Note, however, that there is still some work to do to obtain our Theorem 1.1 from the very general Theorem 3.1.3 of [Suzuki 2018]; compare with Section 4.2 of [loc. cit.], where a similar task is fulfilled for abelian schemes instead of finite group schemes.

the local ring $\mathcal{O}_{X,v}$ of X at v is excellent (indeed $\mathcal{O}_{X,v}$ is either of mixed characteristic or the localization of a ring of finite type over a field); hence so are $\mathcal{O}_v$ (by [EGA IV$_4$ 1967, Corollary 18.7.6]) as the henselization of an excellent ring, and $\hat{\mathcal{O}}_v$ as a complete Noetherian local ring [Matsumura 1970, Section 34].

The piece of notation "$v \notin U$" means that we consider all places v corresponding to closed points of $X \setminus U$ *plus the real places in the number field case*. If v is a real place, we set $K_v = \hat{K}_v = \mathcal{O}_v = \hat{\mathcal{O}}_v$ for the completion of K at v, and we denote by $H^*(K_v, M)$ the *Tate (or modified)* cohomology groups of a $\mathrm{Gal}(\overline{K}_v/K_v)$-module M.

If $\mathcal{F}$ is an fppf sheaf of abelian groups on U, define the Cartier dual $\mathcal{F}^D$ to be the fppf sheaf $\mathcal{F}^D := \underline{\mathrm{Hom}}(\mathcal{F}, \boldsymbol{G}_m)$. Notation as $\Gamma(U, \mathcal{F})$ stands for the group of sections of $\mathcal{F}$ over U, and $\Gamma_Z(U, \mathcal{F})$ for the group of sections that vanish over $U \setminus Z$. If E is a field (e.g., $E = K_v$ or $E = \hat{K}_v$) and $i : \mathrm{Spec}\, E \to U$ is an E-point of U, we will frequently write $H^r(E, \mathcal{F})$ for $H^r(\mathrm{Spec}\, E, i^*\mathcal{F})$. Similarly for an open subset $V \subset U$, the piece of notation $H^r(V, \mathcal{F})$ (resp. $H^r_c(V, \mathcal{F})$) stands for $H^r(V, \mathcal{F}_{|V})$ (resp. $H^r_c(V, \mathcal{F}_{|V})$).

A finite group scheme N over a field E of characteristic $p > 0$ is *local* (or equivalently *infinitesimal*, as in [Demazure and Gabriel 1970, II.4.7.1]) if it is connected (in particular this implies $H^0(E', N) = 0$ for every field extension E' of E). Examples of such group schemes are μ_p (defined by the affine equation $y^p = 1$) and α_p (defined by the equation $y^p = 0$).

Let S be an $\mathbb{F}_p$-scheme. A finite S-group scheme N is of *height 1* if the relative Frobenius map $F_{N/S}$ [Milne 1986, Section III.0] is trivial.

For any topological abelian group A, let $A^* := \mathrm{Hom}_{\mathrm{cont.}}(A, \mathbb{Q}/\mathbb{Z})$ be the group of continuous homomorphisms from A to $\mathbb{Q}/\mathbb{Z}$ (where $\mathbb{Q}/\mathbb{Z}$ is considered as a discrete group) equipped with the compact-open topology. A morphism $f : A \to B$ of topological groups is *strict* if it is continuous, and the restriction $f : A \to f(A)$ is an open map (where the topology on $f(A)$ is induced by B). This is equivalent to saying that f induces an isomorphism of the topological quotient $A/\ker f$ with the topological subspace $f(A) \subset B$.

Concerning sign conventions in homological algebra, we tried to follow the conventions in [Stacks 2005–] throughout the text.

2. Fppf cohomology with compact support

Define

$$Z := X \setminus U \quad \text{and} \quad Z' := \coprod_{v \in Z} \mathrm{Spec}(\hat{K}_v) \ \ \text{(disjoint union)}.$$

Then we have a natural morphism $i : Z' \to U$. Let $\mathcal{F}$ be a sheaf of abelian groups on $(\mathrm{Sch}/U)_{\mathrm{fppf}}$. Let $I^\bullet(\mathcal{F})$ be an injective resolution of $\mathcal{F}$ over U. Denote by $\mathcal{F}_v$ and $I^\bullet(\mathcal{F})_v$ their respective pullbacks to $\mathrm{Spec}\, K_v$, for $v \notin U$.

Given a morphism of schemes $f : T \to S$, the fppf pullback functor f^* is exact (see [Stacks 2005–, Tag 021W, Tag 00XL]) and it admits an exact left adjoint $f_!$ (see [Stacks 2005–, Tag 04CC]), hence f^* maps injective (resp. flasque) objects to injective (resp. flasque) objects. Therefore $I^\bullet(\mathcal{F})_v$ is an injective resolution of $\mathcal{F}_v$.

As noticed by A. Schmidt, the definition of the modified fppf cohomology groups in the number field case in [Milne 1986, III.0.6(a)] has to be written more precisely, because of the noncanonicity of the mapping cone in the derived category. We are grateful to him for the following alternative definition.

Let $\Omega_{\mathbb{R}}$ denote the set of real places of K. For $v \in \Omega_{\mathbb{R}}$, let $a^v : (\mathrm{Sch}\,/\,\mathrm{Spec}(K_v))_{\mathrm{fppf}} \to \mathrm{Spec}(K_v)_{\text{ét}}$ be the natural morphism of sites, where $S_{\text{ét}}$ denotes the small étale site on a scheme S. Since K_v is a perfect field, the direct image functor a^v_* associated to a^v is exact. Hence, by [SGA 4_2 1972, V, Remark 4.6 and Proposition 4.9], the functor a^v_* maps $I^\bullet(\mathcal{F})_v$ to a flasque resolution $a^v_* I^\bullet(\mathcal{F})_v$ of $a^v_*\mathcal{F}_v$. Following [Geisser and Schmidt 2018, Section 2], there is a natural acyclic resolution $D^\bullet(a^v_*\mathcal{F}_v) \to a^v_*\mathcal{F}_v$ of the $\mathrm{Gal}(\overline{K}_v/K_v) = \mathbb{Z}/2\mathbb{Z}$-module $a^v_*\mathcal{F}_v$ (identified with $\mathcal{F}_v(\mathrm{Spec}(\overline{K}_v))$). Splicing the resolutions $D^\bullet(a^v_*\mathcal{F}_v)$ and $a^v_* I^\bullet(\mathcal{F})_v$ together, one gets a complete acyclic resolution $\hat{I}^\bullet(\mathcal{F}_v)$ of the $\mathrm{Gal}(\overline{K}_v/K_v)$-module $a^v_*\mathcal{F}_v$, which computes the Tate cohomology of $a^v_*\mathcal{F}_v$. And by construction, there is a natural morphism $\hat{i}_v : a^v_* I^\bullet(\mathcal{F})_v \to \hat{I}^\bullet(\mathcal{F}_v)$.

As suggested by [Milne 1986, Section III.0], define $\Gamma_c(U, I^\bullet(\mathcal{F}))$ to be the following object in the category of complexes of abelian groups:

$$\Gamma_c(U, I^\bullet(\mathcal{F})) := \mathrm{Cone}\Bigg(\Gamma(U, I^\bullet(\mathcal{F})) \to \Gamma(Z', i^* I^\bullet(\mathcal{F})) \oplus \bigoplus_{v \in \Omega_{\mathbb{R}}} \Gamma(K_v, \hat{I}^\bullet(\mathcal{F}_v))\Bigg)[-1],$$

and $H^r_c(U, \mathcal{F}) := H^r(\Gamma_c(U, I^\bullet(\mathcal{F})))$. We will also denote by $R\Gamma_c(U, \mathcal{F})$ the complex $\Gamma_c(U, I^\bullet(\mathcal{F}))$ viewed in the derived category of fppf sheaves. Observe that in the number field case the groups $H^r_c(U, \mathcal{F})$ may be nonzero even for negative r. In the function field case we have $H^r_c(U, \mathcal{F}) = 0$ for $r < 0$, and also (by Proposition 2.1 below) $H^0_c(U, \mathcal{F}) = 0$ if we assume further $U \neq X$ (the map $H^0(U, \mathcal{F}) \to H^0(\hat{K}_v, \mathcal{F})$ being injective for each $v \notin U$).

From now on, we will abbreviate $\mathrm{Cone}(\cdots)$ by $C(\cdots)$.

Proposition 2.1. (1) *Let $\mathcal{F}$ be a sheaf of abelian groups on U_{fppf}. There is a natural exact sequence, for all $r \geq 0$,*

$$\cdots \to H^r_c(U, \mathcal{F}) \to H^r(U, \mathcal{F}) \to \bigoplus_{v \notin U} H^r(\hat{K}_v, \mathcal{F}) \to H^{r+1}_c(U, \mathcal{F}) \to \cdots.$$

(2) *For any short exact sequence*

$$0 \to \mathcal{F}' \to \mathcal{F} \to \mathcal{F}'' \to 0$$

of sheaves of abelian groups on U, there is a long exact sequence

$$\cdots \to H^r_c(U, \mathcal{F}') \to H^r_c(U, \mathcal{F}) \to H^r_c(U, \mathcal{F}'') \to H^{r+1}_c(U, \mathcal{F}') \to \cdots.$$

(3) *For any flat affine commutative group scheme $\mathcal{F}$ of finite type over U, and any nonempty open subscheme $V \subset U$, there is a canonical exact sequence*

$$\cdots \to H^r_c(V, \mathcal{F}) \to H^r_c(U, \mathcal{F}) \to \bigoplus_{v \in U \setminus V} H^r(\hat{\mathcal{O}}_v, \mathcal{F}) \to H^{r+1}_c(V, \mathcal{F}) \to \cdots,$$

and the following natural diagram commutes:

$$\begin{array}{ccccccc}
 & & \bigoplus_{v\notin V} H^{r-1}(\hat{K}_v,\mathcal{F}) & \xleftarrow{i_2} & \bigoplus_{v\notin U} H^{r-1}(\hat{K}_v,\mathcal{F}) & & \\
 & \nearrow^{i_1} & \downarrow & & \downarrow & & \\
\bigoplus_{v\in U\setminus V} H^{r-1}(\hat{\mathcal{O}}_v,\mathcal{F}) & \longrightarrow & H^r_c(V,\mathcal{F}) & \longrightarrow & H^r_c(U,\mathcal{F}) & \longrightarrow & \bigoplus_{v\in U\setminus V} H^{r}(\hat{\mathcal{O}}_v,\mathcal{F}) \\
 & & \downarrow & & \downarrow & \nearrow & \\
 & & H^r(V,\mathcal{F}) & \xleftarrow{\mathrm{Res}} & H^r(U,\mathcal{F}) & & \\
 & & \downarrow & & \downarrow & & \\
 & & \bigoplus_{v\notin V} H^{r}(\hat{K}_v,\mathcal{F}) & \xrightarrow{\pi} & \bigoplus_{v\notin U} H^{r}(\hat{K}_v,\mathcal{F}) & &
\end{array}$$

where i_1 (*resp.* i_2) *is obtained by putting* 0 *at the places* $v\notin U$ (*resp.* $v\in U\setminus V$) *and* π *is the natural projection.*

(4) *If* $\mathcal{F}$ *is represented by a smooth group scheme, then* $H^r_c(U,\mathcal{F})\cong H^r_{\text{ét},c}(U,\mathcal{F})$ *for* $r\neq 1$, *where* $H^*_{\text{ét},c}$ *stands for modified étale cohomology with compact support* (as defined in [Geisser and Schmidt 2018, Section 2]). *In particular for such* $\mathcal{F}$ *we have* $H^r_c(U,\mathcal{F})\cong H^r_{\text{ét}}(X,j_!\mathcal{F})$ *in the function field case. If in addition the generic fiber* $\mathcal{F}_K$ *is a finite* K*-group scheme, then* $H^1_c(U,\mathcal{F})\cong H^1_{\text{ét},c}(U,\mathcal{F})$ (*which is identified with* $H^1_{\text{ét}}(X,j_!\mathcal{F})$ *in the function field case*).

Remark 2.2. Unlike what happens in étale cohomology, the groups $H^1(\mathcal{O}_v,\mathcal{F})$ and $H^1(\hat{\mathcal{O}}_v,\mathcal{F})$ cannot in general be identified with the group $H^1(k(v),F(v))$, where $k(v)$ is the residue field at v and $F(v)$ the fiber of $\mathcal{F}$ over $k(v)$. For example this already fails for $\mathcal{F}=\mu_p$ and $\hat{\mathcal{O}}_v=\mathbb{F}_p[\![t]\!]$, because by the Kummer exact sequence

$$0\to\mu_p\to\boldsymbol{G}_m\xrightarrow{\cdot p}\boldsymbol{G}_m\to 0$$

in fppf cohomology, the group $H^1(\hat{\mathcal{O}}_v,\mathcal{F})=\hat{\mathcal{O}}_v^*/\hat{\mathcal{O}}_v^{*p}$ is an infinite dimensional $\mathbb{F}_p$-vector space, while $H^1(k(v),F(v))=k(v)^*/k(v)^{*p}=0$. The situation is better for $r\geq 2$ by [Toën 2011, Corollary 3.4]: namely the natural maps from $H^r(\mathcal{O}_v,\mathcal{F})$ and $H^r(\hat{\mathcal{O}}_v,\mathcal{F})$ to $H^r(k(v),F(v))$ are isomorphisms.

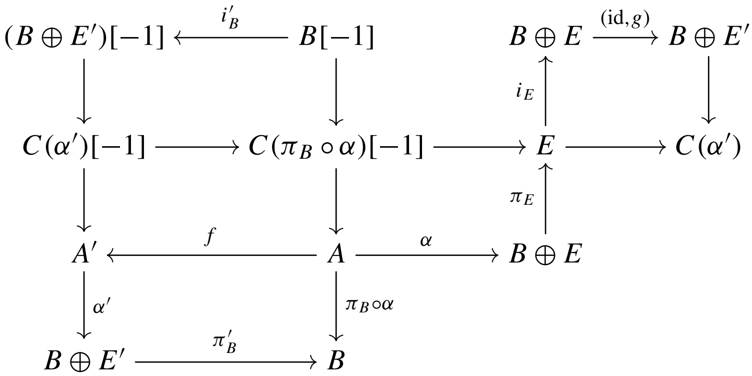
Before proving Proposition 2.1, we need the following lemmas. We start with a lemma in homological algebra.

Lemma 2.3. *Let* $\mathcal{A}$ *be an abelian category with enough injectives and let* $\boldsymbol{C}(\mathcal{A})$ (*resp.* $\boldsymbol{D}(\mathcal{A})$) *denote the category* (*resp. the derived category*) *of bounded below cochain complexes in* $\mathcal{A}$. *Consider a commutative diagram in* $\boldsymbol{C}(\mathcal{A})$:

$$\begin{array}{ccc}
A & \xrightarrow{\alpha} & B\oplus E \\
{\scriptstyle f}\downarrow & & \downarrow{\scriptstyle (\mathrm{id},g)} \\
A' & \xrightarrow{\alpha'} & B\oplus E'
\end{array}$$

and denote by π_B (*resp.* π'_B) *the projection* $B\oplus E\to B$ (*resp.* $B\oplus E'\to B$).

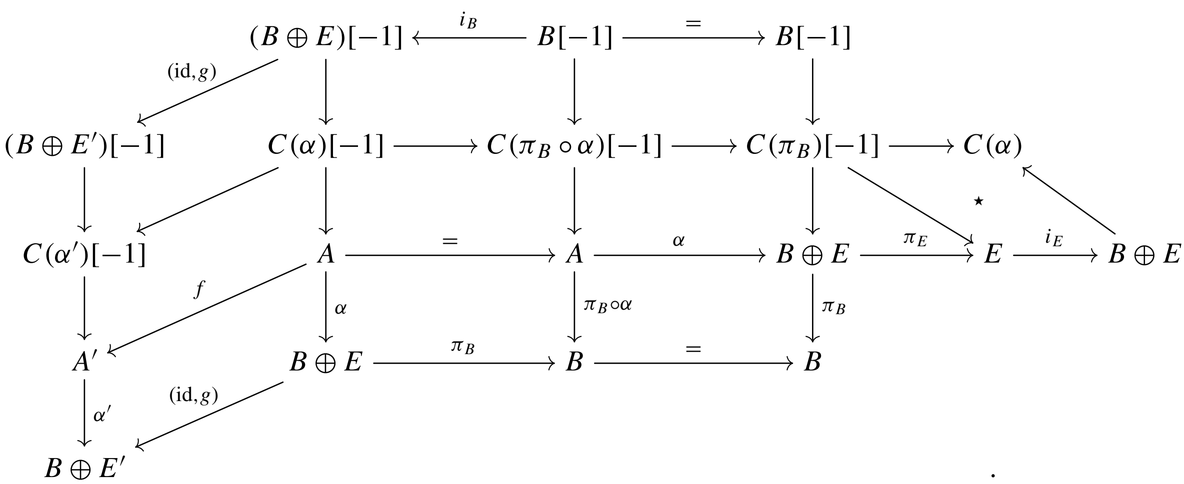
Assume that the natural morphism $C(f) \to C(g)$ in $\boldsymbol{C}(\mathcal{A})$ is a quasi-isomorphism. Then there exists a canonical commutative diagram in $\boldsymbol{D}(\mathcal{A})$:



where the second row and the first two columns are exact triangles.

Proof. The assumption that $C(f) \to C(g) \cong C(\mathrm{Id} \oplus g)$ is a quasi-isomorphism implies that $C(\alpha) \to C(\alpha')$ is a quasi-isomorphism (see for instance Proposition 1.1.11 in [Beilinson et al. 1982] or Corollary A.14 in [Peters and Steenbrink 2008]).

Functoriality of the mapping cone in the category $\boldsymbol{C}(\mathcal{A})$ gives the following diagram in $\boldsymbol{C}(\mathcal{A})$, where the second row (by [Milne 1986, Proposition II.0.10], or [Kashiwara and Schapira 2006, proof of Theorem 11.2.6]) and the columns are exact triangles in the derived category:



As usual, notation as π_B, π_E denotes projections and i_B, i_E are given by putting 0 at the missing piece. Note also that due to our sign conventions, the horizontal map $C(\pi_B)[-1] \to C(\alpha)$ is given by the natural map with a (-1)-sign.

This diagram is commutative in $\boldsymbol{C}(\mathcal{A})$, except the square $\star$ which is commutative up to homotopy. Indeed, this square defines two maps $f, g : C(\pi_B)[-1] \to C(\alpha)$, which are given in degree n by two maps $f^n, g^n : B^{n-1} \oplus (B^n \oplus E^n) \to (B^n \oplus E^n) \oplus A^{n+1}$, where $f^n(b', b, e) := -(b, e, 0)$ and

$g^n(b', b, e) := -(0, e, 0)$. Consider now the maps $s^n : B^{n-1} \oplus (B^n \oplus E^n) \to (B^{n-1} \oplus E^{n-1}) \oplus A^n$ defined by $s^n(b', b, e) := (b', 0, 0)$. Then the collection (s^n) is a homotopy between f and g. Hence the square $\star$ is commutative up to the homotopy (s^n).

Since the map $C(\alpha) \to C(\alpha')$ is a quasi-isomorphism, and since the natural map $C(\pi_B)[-1] \to E$ is a homotopy equivalence, the lemma follows from the commutativity and the exactness of the previous diagram. □

We now need the following result, for which we did not find a suitable reference:

Lemma 2.4. *Let A be a henselian valuation ring with fraction field K. Let $\hat{A}$ be the completion of A for the valuation topology and $\hat{K} := \operatorname{Frac} \hat{A}$. Assume that $\hat{K}$ is separable over K:*

(1) *Let G be a K-group scheme locally of finite type. Then the map $H^1(K, G) \to H^1(\hat{K}, G)$ has dense image.*

(2) *Assume that $\hat{A}$ is henselian. Let G be a flat A-group scheme locally of finite presentation. Then the map $H^1(A, G) \to H^1(\hat{A}, G)$ has dense image.*

Here the topology on the pointed sets $H^1(\hat{A}, G)$ and $H^1(\hat{K}, G)$ is provided by [Česnavičius 2015b, Section 3].

Remarks 2.5.
- The assumption that $\hat{K}$ is separable over K is satisfied if A is an excellent discrete valuation ring.
- In the second statement, the assumption that $\hat{A}$ is henselian is satisfied if the valuation on A has height 1 (special case of [Ribenboim 1968, Section F, Theorem 4]). This assumption is used in the proof below to apply [Česnavičius 2015b, Theorem B.5]. Note also that in general, $\hat{A}$ is not the same as the completion of A for the $\mathfrak{m}$-adic topology (where $\mathfrak{m}$ denotes the maximal ideal of A).

Proof of Lemma 2.4. We prove both statements at the same time. Let E be either A or K, set $S = \operatorname{Spec} E$. Let $\boldsymbol{B}G$ denote the classifying E-stack of G-torsors. We need to prove that $\boldsymbol{B}G(E)$ is dense in $\boldsymbol{B}G(\hat{E})$. It is a classical fact that $\boldsymbol{B}G$ is an algebraic stack [Stacks 2005–, Tag 0CQJ and Tag 06PL]. Let $x \in \boldsymbol{B}G(\hat{E})$ and $U \subset \boldsymbol{B}G(\hat{E})$ be an open subcategory (in the sense of [Česnavičius 2015b, 2.4]) containing x. We need to find an object $x' \in \boldsymbol{B}G(E)$ that maps to $U \subset \boldsymbol{B}G(\hat{E})$. Using [Česnavičius 2015b, Theorem B.5 and Remark B.6] (applied to the S-scheme $\operatorname{Spec} R := \operatorname{Spec} \hat{E}$), there exists an affine scheme Y, a smooth S-morphism $\pi : Y \to \boldsymbol{B}G$ and $y \in Y(\hat{E})$ such that $\pi_{\hat{E}}(y) = x$, where $\pi_{\hat{E}} : Y(\hat{E}) \to \boldsymbol{B}G(\hat{E})$ is the map induced by π. In particular, $Y \to S$ is smooth because so are π and $\boldsymbol{B}G \to S$ (the latter by [Česnavičius 2015b, Proposition A.3]). Hence Y is locally of finite presentation over S. By assumption, $\pi_{\hat{E}}^{-1}(U) \subset Y(\hat{E})$ is an open subset containing y. Hence [Moret-Bailly 2012, Corollary 1.2.1] (in the discrete valuation ring case, it is Greenberg's approximation theorem) implies that $Y(E) \cap \pi_{\hat{E}}^{-1}(U) \neq \varnothing$. Applying π_E, we get that the image of $\boldsymbol{B}G(E)$ meets U, which proves the required result. □

The previous lemma is useful to prove the following crucial (in the function field case) statement. For a local integral domain A with maximal ideal $\mathfrak{m}$, fraction field K and residue field κ, and $\mathcal{F}$ an fppf sheaf on Spec A with an injective resolution $I^\bullet(\mathcal{F})$, define

$$\Gamma_{\mathfrak{m}}(A, I^\bullet(\mathcal{F})) := \mathrm{Cone}(\Gamma(\mathrm{Spec}\, A, I^\bullet(\mathcal{F})) \to \Gamma(\mathrm{Spec}\, K, I^\bullet(\mathcal{F})))[-1]$$

and $H^r_{\mathfrak{m}}(A, \mathcal{F}) := H^r(\Gamma_{\mathfrak{m}}(A, I^\bullet(\mathcal{F})))$ (the cohomology with support in Spec κ). We have a localization long exact sequence [Milne 1986, Proposition III.0.3]

$$\cdots \to H^r_{\mathfrak{m}}(A, \mathcal{F}) \to H^r(A, \mathcal{F}) \to H^r(K, \mathcal{F}) \to H^{r+1}_{\mathfrak{m}}(A, \mathcal{F}) \to \cdots.$$

Lemma 2.6. *Let A be an excellent henselian discrete valuation ring, with maximal ideal $\mathfrak{m}$. Let $\mathcal{F}$ be a flat affine commutative group scheme of finite type over* Spec A. *Then for all $r \geq 0$, the morphism $H^r_{\mathfrak{m}}(A, \mathcal{F}) \to H^r_{\mathfrak{m}}(\hat{A}, \mathcal{F})$ is an isomorphism.*

Remark 2.7. Let $I^\bullet(\mathcal{F})$ be an injective resolution of $\mathcal{F}$ viewed as an fppf sheaf. Another formulation of Lemma 2.6 is that the natural morphism $\Gamma_{\mathfrak{m}}(A, I^\bullet(\mathcal{F})) \to \Gamma_{\mathfrak{m}}(\hat{A}, I^\bullet(\mathcal{F}))$ is an isomorphism in the derived category. The injective resolution $I^\bullet(\mathcal{F})$ can be replaced by any complex of flasque fppf sheaves that is quasi-isomorphic to $\mathcal{F}$ (indeed the fppf pullback functor f^* associated to $f : \mathrm{Spec}\, \hat{A} \to \mathrm{Spec}\, A$ sends flasque resolutions to flasque resolutions, because f^* is exact and preserves flasque sheaves).

Also note that Lemma 2.6 is a variant of [Suzuki 2018, Proposition 2.6.2]: our result is slightly more general in the affine case, while the notion of cohomological approximation in [Suzuki 2018] is a priori a little stronger than the conclusion of Lemma 2.6. In addition, this lemma answers a variant of a question raised after [loc. cit., Proposition 2.6.2] (under a flatness assumption).

Proof of Lemma 2.6. ($r = 0$). Since $\mathcal{F}$ is separated (as an affine scheme), the morphisms $H^0(A, \mathcal{F}) \to H^0(K, \mathcal{F})$ and $H^0(\hat{A}, \mathcal{F}) \to H^0(\hat{K}, \mathcal{F})$ are injective, which implies that

$$H^0_{\mathfrak{m}}(A, \mathcal{F}) = H^0_{\mathfrak{m}}(\hat{A}, \mathcal{F}) = 0.$$

($r = 1$). Consider the following commutative diagram with exact rows:

$$\begin{array}{ccccccccc} H^0(A, \mathcal{F}) & \longrightarrow & H^0(K, \mathcal{F}) & \longrightarrow & H^1_{\mathfrak{m}}(A, \mathcal{F}) & \longrightarrow & H^1(A, \mathcal{F}) & \longrightarrow & H^1(K, \mathcal{F}) \\ \downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\ H^0(\hat{A}, \mathcal{F}) & \longrightarrow & H^0(\hat{K}, \mathcal{F}) & \longrightarrow & H^1_{\mathfrak{m}}(\hat{A}, \mathcal{F}) & \longrightarrow & H^1(\hat{A}, \mathcal{F}) & \longrightarrow & H^1(\hat{K}, \mathcal{F}) \end{array} \tag{1}$$

Since A is excellent, Artin approximation [1969, Theorem 1.12] implies that the morphism $H^1(A, \mathcal{F}) \to H^1(\hat{A}, \mathcal{F})$ is injective: indeed, given a (Spec A)-torsor $\mathcal{P}$ under $\mathcal{F}$, $\mathcal{P}$ is locally of finite presentation, and Artin approximation ensures that $\mathcal{P}(\hat{A}) \neq \varnothing$ implies that $\mathcal{P}(A) \neq \varnothing$.

The affine A-scheme of finite type $\mathcal{F}$ is of the form $\mathrm{Spec}(A[x_1, \ldots, x_n]/(f_1, \ldots, f_r))$, where $f_1, \ldots, f_r$ are polynomials. Since the discrete valuation ring A satisfies $A = K \cap \hat{A} \subset \hat{K}$, the square on the left-hand side in (1) is cartesian.

Hence an easy diagram chase implies that $H^1_{\mathfrak{m}}(A, \mathcal{F}) \to H^1_{\mathfrak{m}}(\hat{A}, \mathcal{F})$ is injective.

By Proposition A.6 in [Gille and Pianzola 2008], the right-hand side square in (1) is cartesian. In addition, $H^0(\hat{A}, \mathcal{F}) \subset H^0(\hat{K}, \mathcal{F})$ is open [Gabber et al. 2014, Proposition 3.3.4], and $H^0(K, \mathcal{F}) \subset H^0(\hat{K}, \mathcal{F})$ is dense by [Gabber et al. 2014, Proposition 3.5.2] (weak approximation for $\mathcal{F}$).

Therefore, an easy diagram chase implies that the map $H^1_{\mathfrak{m}}(A, \mathcal{F}) \to H^1_{\mathfrak{m}}(\hat{A}, \mathcal{F})$ is surjective.

($r = 2$). Consider the commutative diagram with exact rows:

$$\begin{array}{ccccccccc} H^1(A,\mathcal{F}) & \longrightarrow & H^1(K,\mathcal{F}) & \longrightarrow & H^2_{\mathfrak{m}}(A,\mathcal{F}) & \longrightarrow & H^2(A,\mathcal{F}) & \longrightarrow & H^2(K,\mathcal{F}) \\ \downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\ H^1(\hat{A},\mathcal{F}) & \longrightarrow & H^1(\hat{K},\mathcal{F}) & \longrightarrow & H^2_{\mathfrak{m}}(\hat{A},\mathcal{F}) & \longrightarrow & H^2(\hat{A},\mathcal{F}) & \longrightarrow & H^2(\hat{K},\mathcal{F}) \end{array} \tag{2}$$

By [Toën 2011, Corollary 3.4], the map $H^2(A, \mathcal{F}) \to H^2(\hat{A}, \mathcal{F})$ is an isomorphism. And we already explained (in the case $r = 1$) that the left-hand side square in (2) is cartesian. Hence a diagram chase proves that the map $H^2_{\mathfrak{m}}(A, \mathcal{F}) \to H^2_{\mathfrak{m}}(\hat{A}, \mathcal{F})$ is injective.

Using [Gabber et al. 2014, Proposition 3.5.3.(3)], the map $H^2(K, \mathcal{F}) \to H^2(\hat{K}, \mathcal{F})$ is also an isomorphism. By [Česnavičius 2015b, Proposition 2.9(e)], the map $H^1(\hat{A}, \mathcal{F}) \to H^1(\hat{K}, \mathcal{F})$ is open. Lemma 2.4 implies that the map $H^1(K, \mathcal{F}) \to H^1(\hat{K}, \mathcal{F})$ has dense image. By diagram chase, we get that the map $H^2_{\mathfrak{m}}(A, \mathcal{F}) \to H^2_{\mathfrak{m}}(\hat{A}, \mathcal{F})$ is surjective.

($r \geq 3$). Corollary 3.4 in [Toën 2011] implies that the morphisms $H^{r-1}(A, \mathcal{F}) \to H^{r-1}(\hat{A}, \mathcal{F})$ and $H^r(A, \mathcal{F}) \to H^r(\hat{A}, \mathcal{F})$ are isomorphisms. Proposition 3.5.3(3) in [Gabber et al. 2014] implies that the maps $H^{r-1}(K, \mathcal{F}) \to H^{r-1}(\hat{K}, \mathcal{F})$ and $H^r(K, \mathcal{F}) \to H^r(\hat{K}, \mathcal{F})$ are isomorphisms. Therefore, the five-lemma proves that $H^r_{\mathfrak{m}}(A, \mathcal{F}) \to H^r_{\mathfrak{m}}(\hat{A}, \mathcal{F})$ is an isomorphism. □

Remark 2.8. We will apply the previous lemma to a finite and flat commutative group scheme N. As was pointed out to us by K. Česnavičius, it is then possible to argue without using Corollary 3.4 in [Toën 2011] (whose proof is quite involved): indeed there exists [Milne 1986, Theorem III.A.5] an exact sequence

$$0 \to N \to G_1 \to G_2 \to 0$$

of affine A-group schemes such that G_1 and G_2 are smooth. Now for $i > 0$ we have $H^i(A, G_j) \cong H^i(\hat{A}, G_j)$ ($j = 1, 2$) by [Milne 1980, Remark III.3.11], because A and $\hat{A}$ are henselian, and fppf cohomology coincides with étale cohomology for smooth group schemes. It remains to apply the five-lemma to get $H^i(A, N) \cong H^i(\hat{A}, N)$ for $i \geq 2$, which is the input from [Toën 2011] that we used in the proof.

The following lemma is a version of the excision property for fppf cohomology with respect to étale morphisms:

Lemma 2.9. *Let X, X' be schemes, $Z \hookrightarrow X$ (resp. $Z' \hookrightarrow X'$) be closed subschemes, $\pi : X' \to X$ be an étale morphism. Assume that π restricted to Z' is an isomorphism from Z' to Z and that $\pi(X' \setminus Z') \subset X \setminus Z$. Let $\mathcal{F}$ be a sheaf on $(\mathrm{Sch}/X)_{\mathrm{fppf}}$. Then for all $r \geq 0$, the natural morphism $H^r_Z(X, \mathcal{F}) \to H^r_{Z'}(X', \pi^*\mathcal{F})$ is an isomorphism.*

Proof. Since π^* is exact and maps injective objects to injective objects, the proof is exactly the same as the proof of [Milne 1980, Proposition III.1.27]. □

We continue with a lemma comparing the definition of modified étale cohomology with compact support in [Geisser and Schmidt 2018] and our definition of modified fppf cohomology with compact support. For any scheme T, consider the morphisms of sites

$$(\mathrm{Sch}\,/\,T)_{\mathrm{fppf}} \xrightarrow{\varepsilon_T} (\mathrm{Sch}\,/\,T)_{\text{ét}} \xrightarrow{\pi_T} T_{\text{ét}}, \qquad a_T = \pi_T \circ \varepsilon_T$$

where $(\mathrm{Sch}\,/\,T)_{\text{ét}}$ denotes the big étale site of T. Recall that $Z := X \setminus U$, $Z' := \coprod_{v\in Z} \mathrm{Spec}(\hat{K}_v)$, $j : U \to X$ is the open immersion and $i : Z' \to U$ is the natural morphism. Set $a := a_U$ and $\varepsilon := \varepsilon_U$.

Let $\mathcal{F}$ be a sheaf on $U_{\text{ét}}$, and let $\pi_X^* j_! \mathcal{F} \to J^\bullet(\mathcal{F})$ be an injective resolution in the big étale topos of X. By [Stacks 2005–, Tag 0758 and Tag 04BT], the restriction $J^\bullet(\mathcal{F})_{\text{ét}}$ of $J^\bullet(\mathcal{F})$ to the small étale site of X is an injective resolution of $j_!\mathcal{F}$. For every place $v \notin U$ of K, let $\mathcal{F}_v$ be the pull-back of $\mathcal{F}$ to $(\mathrm{Spec}\, K_v)_{\text{ét}}$. As in the fppf case (explained in the beginning of Section 2), we have for v real a complete resolution $\hat{J}^\bullet(\mathcal{F}_v)$ of the $\mathrm{Gal}(\overline{K_v}/K_v)$-module $\mathcal{F}_v$, which computes its Tate cohomology. Following [Geisser and Schmidt 2018, Section 2], we define

$$\Gamma_{\text{ét},c}(U, J^\bullet(\mathcal{F})) := \mathrm{Cone}\Bigl(\Gamma(X, J^\bullet(\mathcal{F})_{\text{ét}}) \to \bigoplus_{v\in\Omega_{\mathbb{R}}} \Gamma(K_v, \hat{J}^\bullet(\mathcal{F}_v))\Bigr)[-1],$$

and $H^r_{\text{ét},c}(U, \mathcal{F}) := H^r(\Gamma_{\text{ét},c}(U, J^\bullet(\mathcal{F})))$.

Denote by $R\Gamma_{\text{ét},c}(U, \mathcal{F})$ the complex $\Gamma_{\text{ét},c}(U, J^\bullet(\mathcal{F}))$ (viewed in the derived category of abelian groups); similarly for v real, set $\widehat{R\Gamma}_{\text{ét}}(K_v, \mathcal{F})$ (resp. $\widehat{R\Gamma}(K_v, a^*\mathcal{F})$) for the complex $\Gamma(K_v, \hat{J}^\bullet(\mathcal{F}_v))$ (resp. $\Gamma(K_v, \hat{I}^\bullet((a^*\mathcal{F})_v))$, where $I^\bullet(a^*\mathcal{F})$ is a flasque resolution of $a^*\mathcal{F}$, compare to the beginning of Section 2) in the derived category of étale sheaves (resp. fppf sheaves) over $\mathrm{Spec}\, K_v$. Finally, let $R\Gamma_{\text{ét},Z}(X, j_!\mathcal{F})$ denote the complex

$$\Gamma_{\text{ét},Z}(X, J^\bullet(\mathcal{F})) := \mathrm{Cone}(\Gamma(X, J^\bullet(\mathcal{F})_{\text{ét}}) \to \Gamma(U, J^\bullet(\mathcal{F})_{\text{ét}}))[-1].$$

Lemma 2.10. (1) *Let $\mathcal{F}$ be a sheaf of abelian groups over $U_{\text{ét}}$. Then there is a canonical commutative diagram in the derived category of abelian groups, where the rows are exact triangles*:

$$\begin{array}{ccccccc}
R\Gamma_{\text{ét},c}(U,\mathcal{F}) & \longrightarrow & R\Gamma_{\text{ét}}(U,\mathcal{F}) & \longrightarrow & R\Gamma_{\text{ét},Z}(X, j_!\mathcal{F})[1] \oplus \bigoplus_{v\in\Omega_{\mathbb{R}}} \widehat{R\Gamma}_{\text{ét}}(K_v,\mathcal{F}) & \longrightarrow & R\Gamma_{\text{ét},c}(U,\mathcal{F})[1] \\
\downarrow & & \downarrow\wr & & \downarrow & & \downarrow \\
R\Gamma_c(U,a^*\mathcal{F}) & \longrightarrow & R\Gamma(U,a^*\mathcal{F}) & \longrightarrow & R\Gamma(Z', i^*a^*\mathcal{F}) \oplus \bigoplus_{v\in\Omega_{\mathbb{R}}} \widehat{R\Gamma}(K_v,a^*\mathcal{F}) & \longrightarrow & R\Gamma_c(U,a^*\mathcal{F})[1]
\end{array}$$

Besides, the complex $R\Gamma_{\text{ét},Z}(X, j_!\mathcal{F})[1]$ is quasi-isomorphic to $\bigoplus_{v\in Z} R\Gamma_{\text{ét}}(K_v, \mathcal{F})$.

(2) *Let G be a smooth commutative group scheme over U. Let $\underline{G}$ denote the fppf sheaf associated to G and $G_{\text{ét}} := a_*\underline{G}$. Then there is a canonical commutative diagram in the derived category of abelian groups, where the rows are exact triangles*:

$$\begin{array}{ccccccc}
R\Gamma_{\text{ét},c}(U, G_{\text{ét}}) & \to & R\Gamma_{\text{ét}}(U, G_{\text{ét}}) & \to & R\Gamma_{\text{ét},Z}(X, j_!G_{\text{ét}})[1] \oplus \bigoplus_{v\in\Omega_{\mathbb{R}}} \widehat{R\Gamma}_{\text{ét}}(K_v, G_{\text{ét}}) & \to & R\Gamma_{\text{ét},c}(U, G_{\text{ét}})[1] \\
\downarrow & & \downarrow \wr & & \downarrow & & \downarrow \\
R\Gamma_c(U, \underline{G}) & \longrightarrow & R\Gamma(U, \underline{G}) & \longrightarrow & R\Gamma(Z', i^*\underline{G}) \oplus \bigoplus_{v\in\Omega_{\mathbb{R}}} \widehat{R\Gamma}(K_v, \underline{G}) & \longrightarrow & R\Gamma_c(U, \underline{G})[1]
\end{array}$$

Besides, the complex $R\Gamma_{\text{ét},Z}(X, j_!G_{\text{ét}})[1]$ is quasi-isomorphic to $\bigoplus_{v\in Z} R\Gamma_{\text{ét}}(K_v, G_{\text{ét}})$.

Proof. (1) Set $J := J^\bullet(\mathcal{F})$. Since $j_!\mathcal{F} \to J_{\text{ét}} := J^\bullet(\mathcal{F})_{\text{ét}}$ is an injective resolution, we get an injective resolution $\mathcal{F} = j^*j_!\mathcal{F} \to j^*J_{\text{ét}}$ in $U_{\text{ét}}$. The functor ε^* is an exact functor that maps flasque étale sheaves to flasque fppf sheaves (see [Stacks 2005–, Tag 0DDU]), we get a flasque resolution $a^*\mathcal{F} \to I := \varepsilon^*j^*J_{\text{ét}}$. Let $\hat{J}_v := \hat{J}^\bullet(\mathcal{F}_v)$; define $\hat{I}_v = \hat{I}^\bullet((\varepsilon^*\mathcal{F})_v)$ (associated to the flasque resolution I of $\varepsilon^*\mathcal{F}$) as in the beginning of Section 2.

Consider now the following commutative diagram of complexes, where $\tilde{\Gamma}_{\text{ét},Z}(U, J)$ and $\tilde{\Gamma}_{\text{ét},c}(U, J)$ are mapping cones defined such that the third and fourth rows are exact triangles:

$$\begin{array}{ccccccc}
\Gamma_{\text{ét},c}(U, J_{\text{ét}}) & \longrightarrow & \Gamma_{\text{ét}}(U, j^*J_{\text{ét}}) & \longrightarrow & \Gamma_{\text{ét},Z}(X, J_{\text{ét}})[1] \oplus \bigoplus_{v\in\Omega_{\mathbb{R}}} \Gamma_{\text{ét}}(K_v, \hat{J}_{\text{ét},v}) & \longrightarrow & \Gamma_{\text{ét},c}(U, J_{\text{ét}})[1] \\
\uparrow \varphi_c & & \uparrow \varphi & & \uparrow \varphi' & & \uparrow \\
\Gamma_{\text{ét},c}(U, J) & \longrightarrow & \Gamma_{\text{ét}}(U, j^*J) & \longrightarrow & \Gamma_{\text{ét},Z}(X, J)[1] \oplus \bigoplus_{v\in\Omega_{\mathbb{R}}} \Gamma_{\text{ét}}(K_v, \hat{J}_v) & \longrightarrow & \Gamma_{\text{ét},c}(U, J)[1] \\
\downarrow d' & & \downarrow = & & \downarrow d & & \downarrow \\
\tilde{\Gamma}_{\text{ét},Z}(U, J) & \longrightarrow & \Gamma_{\text{ét}}(U, j^*J) & \longrightarrow & \bigoplus_{v\in Z} \Gamma_{\text{ét},v}(\mathcal{O}_v, J)[1] \oplus \bigoplus_{v\in\Omega_{\mathbb{R}}} \Gamma_{\text{ét}}(K_v, \hat{J}_v) & \longrightarrow & \tilde{\Gamma}_{\text{ét},Z}(U, J)[1] \\
\uparrow b' & & \uparrow = & & \uparrow b & & \uparrow \\
\tilde{\Gamma}_{\text{ét},c}(U, J) & \longrightarrow & \Gamma_{\text{ét}}(U, j^*J) & \longrightarrow & \bigoplus_{v\in Z} \Gamma_{\text{ét}}(K_v, J) \oplus \bigoplus_{v\in\Omega_{\mathbb{R}}} \Gamma_{\text{ét}}(K_v, \hat{J}_v) & \longrightarrow & \tilde{\Gamma}_{\text{ét},c}(U, J)[1] \\
\downarrow & & \downarrow c & & \downarrow & & \downarrow \\
\Gamma_c(U, I) & \longrightarrow & \Gamma(U, I) & \longrightarrow & \Gamma(Z', i^*I) \oplus \bigoplus_{v\in\Omega_{\mathbb{R}}} \Gamma(K_v, \hat{I}_v) & \longrightarrow & \Gamma_c(U, I)[1]
\end{array}$$

In this diagram, the rows are exact triangles (by definition for the last three rows, using the proof of Lemma 2.7 in [Geisser and Schmidt 2018] for the first ones). The maps φ, φ' and φ_c are quasi-isomorphisms by [Stacks 2005–, Tag 0DDH]. In addition, the maps d and b (hence also d' and b') are quasi-isomorphisms: for the map d, this is the excision property for étale cohomology (see [Milne 1980, Proposition III.1.27]); for the map b, this is exactly [Milne 1986, Proposition II.1.1.(a)]. In addition, the map c is a quasi-isomorphism, using [Stacks 2005–, Tag 0DDU]. This proves the lemma.

(2) Consider the following commutative diagram of exact triangles in the derived category:

$$\begin{array}{ccccccc}
R\Gamma_{\text{ét},c}(U, G_{\text{ét}}) & \longrightarrow & R\Gamma_{\text{ét}}(U, G_{\text{ét}}) & \longrightarrow & R\Gamma_{\text{ét},Z}(X, j_! G_{\text{ét}})[1] \oplus \bigoplus_{v\in\Omega_{\mathbb{R}}} \widehat{R\Gamma_{\text{ét}}}(K_v, G_{\text{ét}}) & \longrightarrow & R\Gamma_{\text{ét},c}(U, G_{\text{ét}})[1] \\
\downarrow & & \downarrow & & \downarrow & & \downarrow \\
R\Gamma_c(U, a^*G_{\text{ét}}) & \longrightarrow & R\Gamma(U, a^*G_{\text{ét}}) & \longrightarrow & R\Gamma(Z', i^*a^*G_{\text{ét}}) \oplus \bigoplus_{v\in\Omega_{\mathbb{R}}} \widehat{R\Gamma}(K_v, a^*G_{\text{ét}}) & \longrightarrow & R\Gamma_c(U, a^*G_{\text{ét}})[1] \\
\downarrow & & \downarrow & & \downarrow & & \downarrow \\
R\Gamma_c(U, \underline{G}) & \longrightarrow & R\Gamma(U, \underline{G}) & \longrightarrow & R\Gamma(Z', i^*\underline{G}) \oplus \bigoplus_{v\in\Omega_{\mathbb{R}}} \widehat{R\Gamma}(K_v, \underline{G}) & \longrightarrow & R\Gamma_c(U, \underline{G})[1]
\end{array}$$

where the vertical maps between the first two rows come from the first point of this lemma, and the ones between the last two rows come from the adjunction morphism $a^*G_{\text{ét}} = a^*a_*\underline{G} \to \underline{G}$ and from the functoriality of the triangle defining the complexes $R\Gamma_c(U, \cdot)$. Now [Grothendieck 1968, Theorem 11.7], ensures that the composed vertical morphism $R\Gamma_{\text{ét}}(U, G_{\text{ét}}) \to R\Gamma(U, \underline{G})$ is an isomorphism. Whence the required result. □

Proof of Proposition 2.1. (1) This is immediate from the definitions.

(2) The claim follows from the definitions, from the exactness of the functors i^*, a_*^v and $D^\bullet(\cdot)$ at the beginning of Section 2, and from the exactness of the cone functor on the category of complexes of abelian groups (see also [Milne 1986, III, Proposition 0.4.a and Remark 0.6.b]).

(3) As in the proof of [Milne 1986, III, Proposition 0.4.c], let $I^\bullet(\mathcal{F})$ be an injective resolution of $\mathcal{F}$. In the number field case, *the piece of notation* $\Gamma(\hat{K}_v, I^\bullet(\mathcal{F}))$ *will stand for* $\Gamma(K_v, \hat{I}^\bullet(\mathcal{F}_v))$ *when* v *is a real place of* K, where $\hat{I}^\bullet(\mathcal{F}_v)$ is the modified resolution constructed in the beginning of Section 2.

Consider the following commutative diagram of complexes in the category of bounded below complexes of abelian groups, where the maps are the natural ones:

$$\begin{array}{ccccc}
\Gamma(U, I^\bullet(\mathcal{F})) & \xrightarrow{\alpha} & \bigoplus_{v\notin U} \Gamma(\hat{K}_v, I^\bullet(\mathcal{F})) \oplus \bigoplus_{v\in U\setminus V} \Gamma(\hat{\mathcal{O}}_v, I^\bullet(\mathcal{F})) & \xrightarrow{\pi_{\mathcal{O}}} & \bigoplus_{v\notin U} \Gamma(\hat{K}_v, I^\bullet(\mathcal{F})) \\
\downarrow{\scriptstyle f} & & \downarrow{\scriptstyle (\mathrm{id}, g)} & \nearrow{\scriptstyle \pi_K} & \\
\Gamma(V, I^\bullet(\mathcal{F})) & \xrightarrow{\alpha'} & \bigoplus_{v\notin U} \Gamma(\hat{K}_v, I^\bullet(\mathcal{F})) \oplus \bigoplus_{v\in U\setminus V} \Gamma(\hat{K}_v, I^\bullet(\mathcal{F})) & &
\end{array}$$

Functoriality of the mapping cone in the category of complexes gives morphisms

$$\Gamma_{U\setminus V}(U, I^\bullet(\mathcal{F})) \to \bigoplus_{v\in U\setminus V} \Gamma_v(\mathcal{O}_v, I^\bullet(\mathcal{F})) \to \bigoplus_{v\in U\setminus V} \Gamma_v(\hat{\mathcal{O}}_v, I^\bullet(\mathcal{F})),$$

where

$$\Gamma_{U\setminus V}(U, I^\bullet(\mathcal{F})) := C(f)[-1], \quad \Gamma_v(\mathcal{O}_v, I^\bullet(\mathcal{F})) := \Gamma_{\mathfrak{m}_v}(\mathcal{O}_v, I^\bullet(\mathcal{F}))$$

and

$$\Gamma_v(\hat{\mathcal{O}}_v, I^\bullet(\mathcal{F})) := \Gamma_{\mathfrak{m}_v}(\hat{\mathcal{O}}_v, I^\bullet(\mathcal{F})).$$

The excision property (Lemma 2.9) implies that the first morphism above $\Gamma_{U\setminus V}(U, I^\bullet(\mathcal{F})) \to \bigoplus_{v\in U\setminus V} \Gamma_v(\mathcal{O}_v, I^\bullet(\mathcal{F}))$ is a quasi-isomorphism.

Since for all $v \in X$, the ring $\mathcal{O}_v$ is an excellent henselian discrete valuation ring, Lemma 2.6 ensures that the second map

$$\bigoplus_{v \in U \setminus V} \Gamma_v(\mathcal{O}_v, I^\bullet(\mathcal{F})) \to \bigoplus_{v \in U \setminus V} \Gamma_v(\hat{\mathcal{O}}_v, I^\bullet(\mathcal{F}))$$

is a quasi-isomorphism. Therefore, the natural morphism $C(f) \to C(g)$ is a quasi-isomorphism.

Apply now Lemma 2.3 to get a commutative diagram in the derived category of abelian groups, where the second row and the first two columns are exact triangles:

$$\begin{array}{ccccccc}
\Big(\bigoplus_{v \notin V} \Gamma(\hat{K}_v, I^\bullet(\mathcal{F}))\Big)[-1] & \xleftarrow{i_K} & \Big(\bigoplus_{v \notin U} \Gamma(\hat{K}_v, I^\bullet(\mathcal{F}))\Big)[-1] & & \bigoplus_{v \notin U} \Gamma(\hat{K}_v, I^\bullet(\mathcal{F})) \oplus \bigoplus_{v \in U \setminus V} \Gamma(\hat{\mathcal{O}}_v, I^\bullet(\mathcal{F})) & \xrightarrow{(\mathrm{id}, g)} & \bigoplus_{v \notin V} \Gamma(\hat{K}_v, I^\bullet(\mathcal{F})) \\
\downarrow & & \downarrow & & \uparrow i'_{\mathcal{O}} & & \downarrow \\
\Gamma_c(V, I^\bullet(\mathcal{F})) & \longrightarrow & \Gamma_c(U, I^\bullet(\mathcal{F})) & \longrightarrow & \bigoplus_{v \in U \setminus V} \Gamma(\hat{\mathcal{O}}_v, I^\bullet(\mathcal{F})) & \longrightarrow & \Gamma_c(V, I^\bullet(\mathcal{F}))[1] \\
\downarrow & & \downarrow & & \uparrow \pi'_{\mathcal{O}} & & \\
\Gamma(V, I^\bullet(\mathcal{F})) & \xleftarrow{f} & \Gamma(U, I^\bullet(\mathcal{F})) & \xrightarrow{\alpha} & \bigoplus_{v \notin U} \Gamma(\hat{K}_v, I^\bullet(\mathcal{F})) \oplus \bigoplus_{v \in U \setminus V} \Gamma(\hat{\mathcal{O}}_v, I^\bullet(\mathcal{F})) & & \\
\downarrow \alpha' & & \downarrow \pi_{\mathcal{O}} \circ \alpha & & & & \\
\bigoplus_{v \notin V} \Gamma(\hat{K}_v, I^\bullet(\mathcal{F})) & \xrightarrow{\pi_K} & \bigoplus_{v \notin U} \Gamma(\hat{K}_v, I^\bullet(\mathcal{F})) & & & &
\end{array} \tag{3}$$

Now the cohomology of this diagram gives the following canonical commutative diagram, with an exact second row (and the two first columns exact):

$$\begin{array}{ccccccc}
\bigoplus_{v \notin V} H^{r-1}(\hat{K}_v, \mathcal{F}) & \leftarrow & \bigoplus_{v \notin U} H^{r-1}(\hat{K}_v, \mathcal{F}) & & \bigoplus_{v \notin U} H^r(\hat{K}_v, \mathcal{F}) \oplus \bigoplus_{v \in U \setminus V} H^r(\hat{\mathcal{O}}_v, \mathcal{F}) & \to & \bigoplus_{v \notin V} H^r(\hat{K}_v, \mathcal{F}) \\
\downarrow & & \downarrow & & \uparrow & & \downarrow \\
\cdots \longrightarrow H^r_c(V, \mathcal{F}) & \longrightarrow & H^r_c(U, \mathcal{F}) & \longrightarrow & \bigoplus_{v \in U \setminus V} H^r(\hat{\mathcal{O}}_v, \mathcal{F}) & \longrightarrow & H^{r+1}_c(V, \mathcal{F}) \longrightarrow \cdots \\
\downarrow & & \downarrow & & \uparrow & & \\
H^r(V, \mathcal{F}) & \xleftarrow{\mathrm{Res}} & H^r(U, \mathcal{F}) & \longrightarrow & \bigoplus_{v \notin U} H^r(\hat{K}_v, \mathcal{F}) \oplus \bigoplus_{v \in U \setminus V} H^r(\hat{\mathcal{O}}_v, \mathcal{F}) & & \\
\downarrow & & \downarrow & & & & \\
\bigoplus_{v \notin V} H^r(\hat{K}_v, \mathcal{F}) & \longrightarrow & \bigoplus_{v \notin U} H^r(\hat{K}_v, \mathcal{F}) & & & &
\end{array}$$

which proves the required exactness and commutativity.

(4) Lemma 2.10 gives a commutative diagram with exact rows:

$$\begin{array}{ccccccccc}
H^{r-1}_{\text{ét}}(U,\mathcal{F}) & \longrightarrow & \bigoplus_{v\notin U} H^{r-1}_{\text{ét}}(K_v,\mathcal{F}) & \longrightarrow & H^r_{\text{ét},c}(U,\mathcal{F}) & \longrightarrow & H^r_{\text{ét}}(U,\mathcal{F}) & \longrightarrow & \bigoplus_{v\notin U} H^r_{\text{ét}}(K_v,\mathcal{F}) \\
\downarrow\wr & & \downarrow & & \downarrow & & \downarrow\wr & & \downarrow \\
H^{r-1}(U,\mathcal{F}) & \longrightarrow & \bigoplus_{v\notin U} H^{r-1}(\hat{K}_v,\mathcal{F}) & \longrightarrow & H^r_c(U,\mathcal{F}) & \longrightarrow & H^r(U,\mathcal{F}) & \longrightarrow & \bigoplus_{v\notin U} H^r(\hat{K}_v,\mathcal{F})
\end{array}$$

Here $H_{\text{ét}}$ stands for étale cohomology (modified over K_v for v real) and $H_{\text{ét},c}$ for (modified) étale cohomology with compact support (as defined in [Geisser and Schmidt 2018, Section 2], or before Lemma 2.10; recall also that in the number field case, the piece of notation $v \notin U$ means that we consider the places corresponding to closed points of $\operatorname{Spec}(\mathcal{O}_K) \setminus U$ *and* the real places).

By [Gabber et al. 2014, Lemma 3.5.3] and [Milne 1980, III.3], we have

$$H^r_{\text{ét}}(K_v,\mathcal{F}) \cong H^r_{\text{ét}}(\hat{K}_v,\mathcal{F}) \xrightarrow{\sim} H^r(\hat{K}_v,\mathcal{F})$$

for all $r \geq 1$ (resp. for all integers r if $\mathcal{F}_K$ is finite; indeed K_v and $\hat{K}_v$ have the same absolute Galois group via [Bourbaki 2006, Section 8, Corollary 4 to Theorem 2], and [Ribenboim 1968, Section F, Corollary 2 to Theorem 2]) and all places v of K. Therefore the five-lemma gives the result. □

Remark 2.11. The definition of fppf compact support cohomology and its related properties are specific to schemes of dimension 1. To the best of our knowledge, there is no good analogue in higher dimension, unlike what happens for étale cohomology.

We will need the following complement to Proposition 2.1:

Proposition 2.12. *Let $\mathcal{F}$ be a flat affine commutative group scheme of finite type over U. Let $V \subset U$ be a nonempty open subset. Then there is a long exact sequence*

$$\cdots \to \bigoplus_{v\in U\setminus V} H^r_v(\hat{\mathcal{O}}_v,\mathcal{F}) \to H^r(U,\mathcal{F}) \to H^r(V,\mathcal{F}) \to \bigoplus_{v\in U\setminus V} H^{r+1}_v(\hat{\mathcal{O}}_v,\mathcal{F}) \to \cdots \tag{4}$$

Proof. The map $\bigoplus_{v\in U\setminus V} H^r_v(\hat{\mathcal{O}}_v,\mathcal{F}) \to H^r(U,\mathcal{F})$ is given by the identification of the first group with $H^r_Z(U,\mathcal{F})$, where $Z = U \setminus V$, via Lemmas 2.6 and 2.9. By the localization exact sequence [Milne 1986, Proposition III.0.3.c], this identification yields the required long exact sequence. □

3. Topology on cohomology groups with compact support

With the previous notation, let us define a natural topology on the groups $H^*_c(U,N)$, where N is a finite flat commutative U-group scheme. Theorem 1.1 actually immediately implies that $H^2_c(U,N)$ is profinite, but this duality theorem will not be used in this paragraph. The "a priori" approach we adopt in this section answers a question raised by Milne [1986, Problem III.8.8].

We restrict ourselves to the function field case, because when K is a number field the groups involved are finite (see [Milne 1986, Theorem III.3.2]; see also Section 5 of this article). Recall that as usual (see for example [Milne 1986, Section III.8]), the groups $H^*(U, N)$ are endowed with the discrete topology. Our first goal in this section is to define a natural topology on the groups $H^*_c(U, N)$.

Given an exact sequence of abelian groups

$$0 \to A \to B \to C \to 0,$$

such that A is a topological group, there exists a unique topology on B such that B is a topological group, A is an open subgroup of B, and C is discrete when endowed with the quotient topology. Indeed, the topology on B is generated by the subsets $b + U$, where $b \in B$ and U is an open subset of A. In addition, given another abelian group B' with a subgroup $A' \subset B'$ that is a topological group, and a commutative diagram of abelian groups

$$\begin{array}{ccc} A & \hookrightarrow & B \\ \downarrow f & & \downarrow g \\ A' & \hookrightarrow & B' \end{array}$$

then f is continuous if and only if g is continuous, for the aforementioned topologies. And f is open if and only if g is.

We can therefore topologize the groups $H^i_c(U, N)$ for $i \neq 2$, using the exact sequence (see Proposition 2.1(1))

$$\bigoplus_{v \notin U} H^{i-1}(\hat{K}_v, N) \to H^i_c(U, N) \to H^i(U, N).$$

Since the groups $H^{i-1}(\hat{K}_v, N)$ are finite for $i \neq 2$ [Milne 1986, Section III.6] and $H^i(U, N)$ is discrete, all groups $H^i_c(U, N)$ are discrete if $i \neq 2$.

Let us now focus on the case $i = 2$. Consider the exact sequence (Proposition 2.1(1))

$$H^1(U, N) \to \bigoplus_{v \notin U} H^1(\hat{K}_v, N) \to H^2_c(U, N) \to H^2(U, N). \tag{5}$$

For $i = 1, 2$, set

$$D^i(U, N) = \operatorname{Im}[H^i_c(U, N) \to H^i(U, N)] = \operatorname{Ker}[H^i(U, N) \to \bigoplus_{v \notin U} H^i(\hat{K}_v, N)].$$

By Proposition 2.1(1), there is an exact sequence

$$\bigoplus_{v \notin U} H^{i-1}(\hat{K}_v, N) \to H^i_c(U, N) \to D^i(U, N) \to 0. \tag{6}$$

The following result has been proved by Česnavičius [2017, Theorem 2.9].[4]

[4]Proposition 2.3 of [loc. cit.] uses the fppf duality Theorem 1.1, but this proposition is actually not needed to prove Theorem 3.1 because a discrete subgroup of a Hausdorff topological group is automatically closed by [Bourbaki 2007, Section 2, Proposition 5]

Theorem 3.1 (Česnavičius). *The map $H^1(U,N) \to \bigoplus_{v\notin U} H^1(\hat{K}_v,N)$ is a strict morphism of topological groups, that is: the image of $H^1(U,N)$ is a discrete subgroup of $\bigoplus_{v\notin U} H^1(\hat{K}_v,N)$. Besides, the group $D^1(U,N)$ is finite.*

Corollary 3.2. *The group $H^1_c(U,N)$ is finite.*

Proof. The group $\bigoplus_{v\notin U} H^0(\hat{K}_v,N)$ is finite (N being a finite U-group scheme). Thus the finiteness of $H^1_c(U,N)$ is equivalent to the finiteness of $D^1(U,N)$ by (6). □

Put the quotient topology on $(\bigoplus_{v\notin U} H^1(\hat{K}_v,N))/\operatorname{Im} H^1(U,N)$. Using Theorem 3.1, the previous facts define a natural topology on $H^2_c(U,N)$, so that morphisms in the exact sequence (5) are continuous (and even strict). This topology makes $H^2_c(U,N)$ a Hausdorff and locally compact group [Bourbaki 2007, Section 2, Proposition 18(a)].

To say more about the topology of $H^2_c(U,N)$, we need a lemma.

Lemma 3.3. (1) *Let $r : N \to N'$ be a morphism of finite flat commutative U-group schemes. Then the corresponding map $s : H^2_c(U,N) \to H^2_c(U,N')$ is continuous. If we assume further that r is surjective, then s is open. If*

$$0 \to N' \to N \to N'' \to 0$$

is an exact sequence of finite flat commutative U-group schemes, then the connecting map $H^2_c(U,N'') \to H^3_c(U,N')$ is continuous.

(2) *Let $V \subset U$ be a nonempty open subset. Then the natural map $u : H^2_c(V,N) \to H^2_c(U,N)$ is continuous.*

Proof. (1) By definition of the topology on the groups H^2_c, it is sufficient to prove that for $v \notin U$, the map $H^1(\hat{K}_v,N) \to H^1(\hat{K}_v,N')$ is continuous (resp. open if r is surjective). Continuity follows from [Česnavičius 2015b, Proposition 4.2] and the openness statement from [Česnavičius 2015b, Proposition 4.3(d)]. Similarly, the last assertion follows from the continuity of the connecting map $H^1(K_v,N'') \to H^2(K_v,N')$ [Česnavičius 2015b, Proposition 4.2] .

(2) Since (by definition of the topology) the image I of $A := \bigoplus_{v\notin V} H^1(\hat{K}_v,N)$ is an open subgroup of $H^2_c(V,N)$, it is sufficient to show that the restriction of u to I is continuous. As I is equipped with the quotient topology (induced by the topology of A), this is equivalent to showing that the natural map $s : A \to H^2_c(U,N)$ is continuous. Now we observe that A is the direct sum of $A_1 := \bigoplus_{v\notin U} H^1(\hat{K}_v,N)$ and $A_2 := \bigoplus_{v\in U\setminus V} H^1(\hat{K}_v,N)$. The restriction of s to A_1 is continuous by the commutative diagram of Proposition 2.1(3). Therefore it only remains to show that the restriction s_2 of s to A_2 is continuous. By [loc. cit.], the restriction of s_2 to $\bigoplus_{v\in U\setminus V} H^1(\hat{\mathcal{O}}_v,N)$ is zero. Since $\bigoplus_{v\in U\setminus V} H^1(\hat{\mathcal{O}}_v,N)$ is an open subgroup of $\bigoplus_{v\in U\setminus V} H^1(\hat{K}_v,N)$ [Česnavičius 2015b, Proposition 3.10], the result follows. □

Recall also the following (probably well-known) lemma:

Lemma 3.4. *Let $f : A \to B$ be a continuous morphism of topological groups, with B Hausdorff*:

(1) *Assume that A is profinite. Then f is strict.*

(2) *Assume that f is injective and A is compact. Then f is strict.*

(3) *Let*

$$0 \to A \xrightarrow{i} B \xrightarrow{\pi} C \to 0$$

be an exact sequence of topological groups with i strict and π continuous. If A and C are completely disconnected, then so is B.

Proof. (1) Since f is continuous and B Hausdorff, the image of f is a compact subspace of B, so we can assume that B is compact and f is onto. The topology of A has a basis consisting of open subgroups, so it is sufficient to show that the image of such a subgroup U is open. As U is closed (hence compact) and of finite index in A, its image $f(U)$ is also compact and of finite index in B, hence it is an open subgroup of B.

(2) Since A is compact and B is Hausdorff, we get that i is a closed map (because the image of a compact subspace of A is compact), hence it induces a homeomorphism from i onto the subspace $i(A) \subset B$. This means that i is strict.

(3) Let D be a connected subset of B. Then $\pi(D)$ is connected, hence is a singleton. Thus, by translating, one can assume that $D \subset i(A)$; as i is strict, the subset $i^{-1}(D) \subset A$ is connected, so it is reduced to a point, hence D is a singleton. This proves the statement. □

Proposition 3.5. *For every integer i with $0 \le i \le 3$, the topology on $H^i_c(U, N)$ is profinite.*

Proof. The only nontrivial case is $i = 2$. We first observe that if there is an exact sequence of finite flat commutative U-group schemes

$$0 \to N' \to N \to N'' \to 0,$$

then it is sufficient to prove that $H^2_c(U, N')$ and $H^2_c(U, N'')$ are profinite to get the same result for $H^2_c(U, N)$. Indeed by Proposition 2.1, 3., there is an exact sequence

$$H^1_c(U, N'') \to H^2_c(U, N') \to H^2_c(U, N) \to H^2_c(U, N'').$$

The group $H^1_c(U, N'')$ is finite by Corollary 3.2; besides, all maps are continuous and the map $H^2_c(U, N) \to H^2_c(U, N'')$ is open (in particular it is strict, and its image is profinite as soon as $H^2_c(U, N'')$ is) by Lemma 3.3(1). Therefore if $H^2_c(U, N')$ and $H^2_c(U, N'')$ are profinite, then $H^2_c(U, N)$ is profinite as an extension

$$0 \xrightarrow{i} A \to H^2_c(U, N) \xrightarrow{\pi} B \to 0$$

of two profinite groups A, B such that the map π is open (the map i is strict by Lemma 3.4, 2.; the group $H^2_c(U, N)$ is completely disconnected by Lemma 3.4 3., and its compactness follows from the fact that π is a proper map by [Bourbaki 2007, Section 4, Corollary 2 to Proposition 2]).

This being said, note now that Proposition 2.1(4) implies the result when the order of N is prime to p by [Milne 1986, Corollary II.3.3] (in this case $H^2_c(U,N)$ is even finite). One can therefore assume by devissage that the order of N is a power of p. The generic fiber N_K of N is a finite commutative group scheme over K. By [Demazure and Gabriel 1970, IV, Section 3.5], N_K admits a composition series whose quotients are étale (with a dual of height one), local (of height one) with étale dual, or α_p. The schematic closure in N of this composition series provides a composition series defined over U. Thus, using the same devissage argument as above, one reduces to the case where the generic fiber N_K or its dual N_K^D has height one.

Proposition III.B.4 and Corollary III.B.5 in [Milne 1986] now imply that there exists a nonempty open subset $V \subset U$ such that $N_{|V}$ extends to a finite flat commutative group scheme $\tilde{N}$ over the proper k-curve X.

Then Proposition 2.1(3) gives an exact sequence

$$H^1_c(X,\tilde{N}) \to \bigoplus_{v\in X\setminus V} H^1(\hat{\mathcal{O}}_v,\tilde{N}) \to H^2_c(V,N) \to H^2_c(X,\tilde{N}) \tag{7}$$

and since we are in the function field case with X proper over k, we have $H^i_c(X,\tilde{N}) = H^i(X,\tilde{N})$ for every positive integer i.

By Proposition 2.1(3), the map $\bigoplus_{v\in X\setminus V} H^1(\hat{\mathcal{O}}_v,\tilde{N}) \to H^2_c(V,N)$ factors through $\bigoplus_{v\in X\setminus V} H^1(\hat{K}_v,N)$, hence it is continuous. By Lemma 3.3, all maps in (7) are continuous. In addition, the groups $H^1_c(X,\tilde{N}) = H^1(X,\tilde{N})$ and $H^2_c(X,\tilde{N}) = H^2(X,\tilde{N})$ are finite by [Milne 1986, Lemma III.8.9]. Besides, $\bigoplus_{v\in X\setminus V} H^1(\hat{\mathcal{O}}_v,\tilde{N})$ is profinite by [loc. cit, Section III.7]; hence $H^2_c(V,N)$ is profinite as an extension (the maps being strict by Lemma 3.4(2)) of a finite group by a profinite group.

Since $H^2(\hat{\mathcal{O}}_v,N) = 0$ for every $v \in U$ [Milne 1986, Section III.7], Proposition 2.1(3) gives an exact sequence of groups

$$\bigoplus_{v\in U\setminus V} H^1(\hat{\mathcal{O}}_v,N) \to H^2_c(V,N) \to H^2_c(U,N) \to 0,$$

which implies that $H^2_c(U,N)$ is profinite, the map $H^2_c(V,N) \to H^2_c(U,N)$ being continuous by Lemma 3.3(2), hence strict by Lemma 3.4(1), because $H^2_c(V,N)$ is profinite and $H^2_c(U,N)$ is Hausdorff. □

The following statement will be useful in the next section:

Proposition 3.6. *Assume that $\mathcal{F} = N$, $\mathcal{F}' = N'$ and $\mathcal{F}'' = N''$ are finite and flat commutative group schemes over U. Then all the maps in Proposition 2.1 are strict (in particular continuous).*

Proof. For the maps in assertion 1 of Proposition 2.1, this follows from the definition of the topology and Theorem 3.1.

Let us consider the maps in assertion 2. The finiteness of the H^1_c groups (Corollary 3.2) implies that it only remains to deal with the maps between H^2_c's and the connecting map $H^2_c(U,\mathcal{F}'') \to H^3_c(U,\mathcal{F}')$. All these maps are continuous by Lemma 3.3, hence strict by Lemma 3.4 1. and Proposition 3.5.

Finally, it has already been proven (see the proof of Proposition 3.5) that the maps in the exact sequence of assertion 3 are continuous. They are strict via Lemma 3.4(1) because $H^1_c(U,\mathcal{F})$ is finite, $H^2_c(U,\mathcal{F})$ (resp. $\bigoplus_{v\in U\setminus V} H^1(\hat{\mathcal{O}}_v,\mathcal{F})$) is profinite, and the other groups are discrete. □

4. Proof of Theorem 1.1 in the function field case

In this section K is the function field of a projective, smooth and geometrically integral curve X defined over a finite field k of characteristic p. The proof follows the same lines as the proof of [Milne 1986, Theorem III.8.2], replacing Proposition III.0.4 in [Milne 1986] by Proposition 2.1 and using the results of Section 2.

For every nonempty open subset $V\subset U$, the natural map $H^3_c(V,\boldsymbol{G}_m)\xrightarrow{s}H^3_c(U,\boldsymbol{G}_m)$ is an isomorphism, and the trace map identifies $H^3_c(U,\boldsymbol{G}_m)$ with $\mathbb{Q}/\mathbb{Z}$ (this identification being compatible with s). Indeed since $\boldsymbol{G}_m$ is a smooth group scheme we can apply Proposition 2.1(4) and [Milne 1986, Section II.3].

For an fppf sheaf $\mathcal{F}$ on U, let us first define the pairing of abelian groups

$$H^{3-r}_c(U,\mathcal{F})\times H^r(U,\mathcal{F}^D)\to H^3_c(U,\boldsymbol{G}_m)\cong\mathbb{Q}/\mathbb{Z}.$$

Since the cohomology groups with compact support are defined via a mapping cone construction, we need to construct this pairing carefully at the level of complexes in order to be able to prove the compatibilities that follow (see Lemmas 4.3 and 4.7 for instance).

Lemma 4.1. *Let A and B be two fppf sheaves of abelian groups on U. Then there exists a canonical pairing in the derived category of abelian groups*

$$R\Gamma_c(U,A)\otimes^{\boldsymbol{L}}R\Gamma(U,B)\to R\Gamma_c(U,A\otimes B).$$

Moreover, this pairing is functorial in A and B.

Proof. For any complex C of fppf sheaves, let $G(C)$ denote the Godement resolution of C (see for instance [SGA 4_3 1973, XVII, 4.2.9]; Godement resolutions exist on the big fppf site because this site has enough points, see Remark 1.6 of [Gabber and Kelly 2015] or [Stacks 2005–, Tag 06VX]).

Then there is a commutative diagram of complexes of sheaves (see [Godement 1958, II.6.6] or [Friedlander and Suslin 2002, Appendix A]):

$$\begin{array}{ccc} A\otimes B & & \\ \downarrow & \searrow & \\ \mathrm{Tot}(G(A)\otimes G(B)) & \longrightarrow & G(A\otimes B) \end{array}$$

The horizontal morphism induces a morphism of complexes of abelian groups

$$\mathrm{Tot}(\Gamma(U,G(A))\otimes\Gamma(U,G(B)))\to\Gamma(U,G(A\otimes B))$$

hence a canonical morphism in the derived category of abelian groups

$$\Gamma(U, G(A)) \otimes^{\boldsymbol{L}} \Gamma(U, G(B)) \to \Gamma(U, G(A \otimes B)).$$

Considering the local versions of the previous pairings, one gets a commutative diagram of complexes of abelian groups

$$\begin{array}{ccc} \mathrm{Tot}(\Gamma(U, G(A)) \otimes \Gamma(U, G(B))) & \longrightarrow & \Gamma(U, G(A \otimes B)) \\ \downarrow & & \downarrow \\ \prod_{v \notin U} \mathrm{Tot}(\Gamma(\hat{K}_v, G(A)) \otimes \Gamma(U, G(B))) & \longrightarrow & \prod_{v \notin U} \Gamma(\hat{K}_v, G(A \otimes B)) \end{array}$$

and functoriality of cones gives a canonical morphism of complexes (via Proposition A.1 in the Appendix)

$$\mathrm{Tot}(\Gamma_c(U, G(A)) \otimes \Gamma(U, G(B))) \to \Gamma_c(U, G(A \otimes B)). \tag{8}$$

Since Godement resolutions are acyclic (see [SGA 4_3 1973, XVII, Proposition 4.2.3]), we know that $R\Gamma(U, C) \cong \Gamma(U, G(C))$ in the derived category, for any fppf sheaf C. Hence the pairing (8) gives the required morphism in the derived category

$$R\Gamma_c(U, A) \otimes^{\boldsymbol{L}} R\Gamma(U, B) \to R\Gamma_c(U, A \otimes B).$$

The functoriality of Godement resolutions implies the functoriality of the pairing in A and B. □

Using Lemma 4.1, [Stacks 2005–, Tag 068G] gives a natural pairing

$$H^r_c(U, A) \times H^s(U, B) \to H^{r+s}_c(U, A \otimes B),$$

whence we deduce the required canonical pairings, for any sheaf $\mathcal{F}$ on $(\mathrm{Sch}/U)_{\mathrm{fppf}}$

$$H^r_c(U, \mathcal{F}) \times H^s(U, \mathcal{F}^D) \to H^{r+s}_c(U, \boldsymbol{G}_m), \tag{9}$$

using the canonical map $\mathcal{F} \otimes \mathcal{F}^D = \mathcal{F} \otimes \underline{\mathrm{Hom}}(\mathcal{F}, \boldsymbol{G}_m) \to \boldsymbol{G}_m$.

Let us describe explicitly the pairing above: the map

$$\mathrm{Tot}(\Gamma_c(U, G(A)) \otimes \Gamma(U, G(B))) \to \Gamma_c(U, G(A \otimes B))$$

is given by maps

$$\Big(\prod_{v \notin U} \Gamma(\hat{K}_v, G_{r-1}(A)) \oplus \Gamma(U, G_r(A))\Big) \otimes \Gamma(U, G_s(B)) \to \prod_{v \notin U} \Gamma(\hat{K}_v, G_{r+s-1}(A \otimes B)) \oplus \Gamma(U, G_{r+s}(A \otimes B))$$
$$(a_{r-1}, a_r) \otimes b_s \mapsto (a_{r-1} \cup \beta(b_s), a_r \cup b_s),$$

where the maps denoted by $\cup$ are the natural pairings, and $\beta : \Gamma(U, G_s(B)) \to \prod_{v \notin U} \Gamma(\hat{K}_v, G_s(B))$ is the localization map.

In the following, we will need an alternative version of the above pairing: with the same notation as above, one defines a pairing in the derived category

$$R\Gamma(U, A) \otimes^{L} R\Gamma_c(U, B) \to R\Gamma_c(U, A \otimes B).$$

The definition is similar to the one in Lemma 4.1: the commutative diagram of complexes

$$\begin{array}{ccc} \mathrm{Tot}(\Gamma(U, G(A)) \otimes \Gamma(U, G(B))) & \longrightarrow & \Gamma(U, G(A \otimes B)) \\ \downarrow & & \downarrow \\ \prod_{v \notin U} \mathrm{Tot}(\Gamma(U, G(A)) \otimes \Gamma(\hat{K}_v, G(B))) & \longrightarrow & \prod_{v \notin U} \Gamma(\hat{K}_v, G(A \otimes B)) \end{array}$$

and Proposition A.1 in the Appendix gives a morphism of complexes

$$\mathrm{Tot}(\Gamma(U, G(A)) \otimes \Gamma_c(U, G(B))) \to \Gamma_c(U, G(A \otimes B)). \tag{10}$$

Taking into account the signs in Proposition A.1, one can describe the pairing $\mathrm{Tot}(\Gamma(U, G(A)) \otimes \Gamma_c(U, G(B))) \to \Gamma_c(U, G(A \otimes B))$ explicitly as follows:

$$\Gamma(U, G_r(A)) \otimes \Big(\prod_{v \notin U} \Gamma(\hat{K}_v, G_{s-1}(B)) \oplus \Gamma(U, G_s(B)) \Big) \to \prod_{v \notin U} \Gamma(\hat{K}_v, G_{r+s-1}(A \otimes B)) \oplus \Gamma(U, G_{r+s}(A \otimes B))$$
$$a_r \otimes (b_{s-1}, b_s) \mapsto ((-1)^r \alpha(a_r) \cup b_{s-1}, a_r \cup b_s),$$

where $\alpha : \Gamma(U, G_r(A)) \to \prod_{v \notin U} \Gamma(\hat{K}_v, G_r(A))$ is the localization map.

We now compare the two pairings defined above:

Lemma 4.2. *The following diagram of complexes commutes up to homotopy*:

$$\begin{array}{ccc} \mathrm{Tot}(\Gamma_c(U, G(A)) \otimes \Gamma(U, G(B))) & \longrightarrow & \Gamma_c(U, G(A \otimes B)) \\ {=}\uparrow \qquad \uparrow & & \\ \mathrm{Tot}(\Gamma_c(U, G(A)) \otimes \Gamma_c(U, G(B))) & & \Big\downarrow {=} \\ \downarrow \qquad \downarrow{=} & & \\ \mathrm{Tot}(\Gamma(U, G(A)) \otimes \Gamma_c(U, G(B))) & \longrightarrow & \Gamma_c(U, G(A \otimes B)) \end{array}$$

Proof. Using the explicit descriptions above, one needs to prove that the map $\varphi_{r,s}$ from

$$\Big(\prod_{v \notin U} \Gamma(\hat{K}_v, G_{r-1}(A)) \oplus \Gamma(U, G_r(A)) \Big) \otimes \Big(\prod_{v \notin U} \Gamma(\hat{K}_v, G_{s-1}(B)) \oplus \Gamma(U, G_s(B)) \Big)$$

to

$$\prod_{v \notin U} \Gamma(\hat{K}_v, G_{r+s-1}(A \otimes B)) \oplus \Gamma(U, G_{r+s}(A \otimes B))$$

given by

$$(a_{r-1}, a_r) \otimes (b_{s-1}, b_s) \mapsto ((-1)^r \alpha(a_r) \cup b_{s-1} - a_{r-1} \cup \beta(b_s), 0)$$

is homotopically trivial. To prove this, consider the maps

$$\Big(\prod_{v\notin U}\Gamma(\hat{K}_v, G_{r-1}(A))\oplus\Gamma(U, G_r(A))\Big)\otimes\Big(\prod_{v\notin U}\Gamma(\hat{K}_v, G_{s-1}(B))\oplus\Gamma(U, G_s(B))\Big) \xrightarrow{h_{r,s}} \prod_{v\notin U}\Gamma(\hat{K}_v, G_{r+s-2}(A\otimes B))\oplus\Gamma(U, G_{r+s-1}(A\otimes B))$$

given by $h_{r,s} : (a_{r-1}, a_r)\otimes(b_{s-1}, b_s)\mapsto(0, (-1)^r a_{r-1}\cup b_{s-1})$. Then these maps define an homotopy equivalence between the map $\bigoplus_{r+s=n}\varphi_{r,s}$ and the zero map, proving the lemma. □

We now prove that the pairing is compatible with coboundary maps in cohomology coming from short exact sequences:

Lemma 4.3. *Let $0\to A\to B\to C\to 0$ and $0\to C'\to B'\to A'\to 0$ be two exact sequences of fppf sheaves on U, and let $B\otimes B'\to D$ be a morphism of fppf sheaves. Assume that the induced morphism $A\otimes C'\to D$ is trivial.*

Consider the following diagram

$$\begin{array}{ccccc} H^r_c(U, C) \times H^{s+1}(U, C') & \xrightarrow{\cup} & H^{r+s+1}_c(U, D) \\ \downarrow \partial_r \qquad\qquad \uparrow \partial'_s & & \downarrow = \\ H^{r+1}_c(U, A) \times H^{s}(U, A') & \xrightarrow{\cup} & H^{r+s+1}_c(U, D) \end{array}$$

where the horizontal morphisms are induced by the pairings in Lemma 4.1 and by the morphism $B\otimes B'\to D$, and the vertical maps are the coboundary morphisms.

Then for all $c\in H^r_c(U, C)$ and $a'\in H^s(U, A')$, we have

$$\partial_r(c)\cup a' + (-1)^r c\cup\partial'_s(a') = 0.$$

Proof. For all fppf sheaves E, let $\partial^E_i : G_i(E)\to G_{i+1}(E)$ denote the coboundary map in the Godement complex $G(E)$.

Consider the diagram induced by $B\otimes B'\to D$

$$\begin{array}{ccccc} \Gamma(U, G_r(B))\otimes\Gamma(U, G_{s+1}(B')) & \xrightarrow{\cup} & \Gamma(U, G_{r+s+1}(D)) \\ \downarrow \partial^B_r \qquad\qquad \uparrow \partial^{B'}_s & & \downarrow = \\ \Gamma(U, G_{r+1}(B))\otimes\Gamma(U, G_{s}(B')) & \xrightarrow{\cup} & \Gamma(U, G_{r+s+1}(D)) \end{array}$$

together with the similar diagrams over Spec $\hat{K}_v$, for all $v\notin S$.

By compatibility of the Godement resolution with tensor product [Friedlander and Suslin 2002, Appendix A], the pairing $\mathrm{Tot}(G(B)\otimes G(B'))\to G(D)$ is a morphism of complexes. Hence for all $b\in\Gamma(U, G_r(B))$ and $b'\in\Gamma(U, G_s(B'))$, we have

$$\partial^B_r(b)\cup b' + (-1)^r b\cup\partial^{B'}_s(b') = \partial^D_{r+s}(b\cup b').$$

This formula, its analogue over Spec $\hat{K}_v$ for $v \notin S$, together with the definition of the connecting maps in cohomology via Godement resolutions (recall that for all n, the functor $\mathcal{F} \mapsto G_n(\mathcal{F})$ is exact, see [SGA 4_3 1973, XVII, Proposition 4.2.3]), implies Lemma 4.3. □

Lemma 4.4. *Let N be a finite flat commutative U-group scheme of order n, then the pairings (9)*

$$H_c^r(U, N) \times H^s(U, N^D) \to H_c^{r+s}(U, \mu_n)$$

are continuous.

Proof. The pairings (9) are defined via the cup-product on U and the local duality pairings $H^a(\hat{K}_v, N) \times H^b(\hat{K}_v, N^D) \to H^{a+b}(\hat{K}_v, \mu_n)$. These local pairings are continuous [Česnavičius 2015b, Theorems 5.11 and 6.5]. Hence the lemma follows from the definition of the topologies on the cohomology groups (see Section 3). □

Remark 4.5. In [Milne 1986] (see for example Theorem III.3.1), the pairings are defined via the Ext groups, which is quite convenient for the definition itself but makes the required commutativities of diagrams more difficult to check. Nevertheless, Proposition V.1.20 in [Milne 1980] provides a similar comparison between both definitions: see the details in Proposition A.2 of the Appendix.

In order to prove Theorem 1.1, we now need to show that the induced map $H_c^{3-r}(U, N) \to H^r(U, N^D)^*$ is an isomorphism (of topological groups) for every finite flat commutative group scheme N over U and every $r \in \{0, 1, 2, 3\}$ (recall that the groups $H^r(U, N^D)$ are equipped with the discrete topology).

We first recall the following lemma [Milne 1986, Lemma III.8.3]:

Lemma 4.6. *Let*

$$0 \to N' \to N \to N'' \to 0$$

be an exact sequence of finite flat commutative group schemes over U. If Theorem 1.1 is true for N' and N'', then it is true for N.

Proof. Using Proposition 2.1(2), the exactness of Pontryagin duality for discrete groups and the pairing in Lemma 4.1, one gets a diagram of long exact sequences:

$$\begin{array}{ccccccccc}
\cdots \longrightarrow & H_c^{3-r}(U, N') & \longrightarrow & H_c^{3-r}(U, N) & \longrightarrow & H_c^{3-r}(U, N'') & \longrightarrow \cdots \\
\star & \downarrow & & \downarrow & & \downarrow & \star \\
\cdots \longrightarrow & H^r(U, N'^D)^* & \longrightarrow & H^r(U, N^D)^* & \longrightarrow & H^r(U, N''^D)^* & \longrightarrow \cdots
\end{array}$$

The functoriality of the pairing (see Lemma 4.1) implies that both central squares in the diagram are commutative. Lemma 4.3 implies that both extreme squares (denoted $\star$) are commutative up to sign. By Lemma 3.4(1), Proposition 3.6 and Lemma 4.4, all the maps in this diagram are continuous. Hence the lemma follows from the five-lemma. □

We now want to show that it is sufficient to prove Theorem 1.1 for a smaller open subset $V \subset U$. To do this, we need to check the compatibility of the pairing in Theorem 1.1 with restriction to an open subset of U and with the local duality pairing (see Lemma 4.7 below).

We first define the maps that appear in this lemma. Let $\mathcal{F}$ be a flat affine commutative U-group scheme of finite type and let $V \subset U$ be a nonempty open subset. Let W denote $U \setminus V$. In diagram (11) below, the first column is the long exact sequence of Proposition 2.1(3), and the second column is the localization exact sequence from Proposition 2.12. The horizontal pairings are either the local duality pairings from [Milne 1986, Theorem III.7.1] (first and last rows), using the same sign convention as in the pairing (10), or the global pairings from Lemma 4.1 (second and third rows). The proof of Proposition 2.12 provides an isomorphism $H^3_W(U, \boldsymbol{G}_m) \cong \bigoplus_{v\in W} H^3_v(\hat{\mathcal{O}}_v, \boldsymbol{G}_m)$, and the natural morphism of complexes $\Gamma_W(U, \boldsymbol{I}^\bullet(\boldsymbol{G}_m)) \to \Gamma_c(V, \boldsymbol{I}^\bullet(\boldsymbol{G}_m))$ gives a morphism $H^3_W(U, \boldsymbol{G}_m) \to H^3_c(V, \boldsymbol{G}_m)$, whence natural morphisms $\bigoplus_{v\in W} H^3_v(\hat{\mathcal{O}}_v, \boldsymbol{G}_m) \to H^3_c(V, \boldsymbol{G}_m) \to H^3_c(U, \boldsymbol{G}_m)$.

Lemma 4.7. *Let $\mathcal{F}$, $\mathcal{G}$ be flat affine commutative group schemes of finite type on U, together with a pairing $\mathcal{F} \otimes \mathcal{G} \to \boldsymbol{G}_m$. Let $V \subset U$ be a nonempty open subscheme and $W := U \setminus V$. Then the following diagram is commutative*:

$$
\begin{array}{ccccc}
\bigoplus_{v\in W} H^{2-r}(\hat{\mathcal{O}}_v, \mathcal{F}) & \times & \bigoplus_{v\in W} H^{r+1}_v(\hat{\mathcal{O}}_v, \mathcal{G}) & \longrightarrow & \bigoplus_{v\in W} H^3_v(\hat{\mathcal{O}}_v, \boldsymbol{G}_m) \\
\downarrow & & \uparrow & & \downarrow \\
H^{3-r}_c(V, \mathcal{F}) & \times & H^r(V, \mathcal{G}) & \longrightarrow & H^3_c(V, \boldsymbol{G}_m) \\
\downarrow & & \uparrow & & \downarrow \wr \\
H^{3-r}_c(U, \mathcal{F}) & \times & H^r(U, \mathcal{G}) & \longrightarrow & H^3_c(U, \boldsymbol{G}_m) \\
\downarrow & & \uparrow & & \uparrow \\
\bigoplus_{v\in W} H^{3-r}(\hat{\mathcal{O}}_v, \mathcal{F}) & \times & \bigoplus_{v\in W} H^{r}_v(\hat{\mathcal{O}}_v, \mathcal{G}) & \longrightarrow & \bigoplus_{v\in W} H^3_v(\hat{\mathcal{O}}_v, \boldsymbol{G}_m)
\end{array}
\tag{11}
$$

In addition, if $\mathcal{F}$ and $\mathcal{G}$ are finite and flat group schemes, then all the maps in the diagram are continuous.

Proof. (1) We first prove the commutativity of the top rectangle. It is sufficient to prove that the following diagram commutes:

$$
\begin{array}{ccc}
\mathrm{Tot}\big(\bigoplus_{v\in W} \Gamma(\hat{\mathcal{O}}_v, G(\mathcal{F}))[-1] \otimes \bigoplus_{v\in W} \Gamma_v(\hat{\mathcal{O}}_v, G(\mathcal{G}))[1]\big) & \longrightarrow & \bigoplus_{v\in W} \Gamma_v(\hat{\mathcal{O}}_v, G(\boldsymbol{G}_m)) \\
\downarrow \qquad \uparrow & & \uparrow \\
\mathrm{Tot}\big(\bigoplus_{v\in W} \Gamma(\hat{K}_v, G(\mathcal{F}))[-1] \otimes \bigoplus_{v\in W} \Gamma(\hat{K}_v, G(\mathcal{G}))\big) & \longrightarrow & \bigoplus_{v\in W} \Gamma(\hat{K}_v, G(\boldsymbol{G}_m))[-1] \\
\downarrow \qquad \uparrow & & \downarrow \\
\mathrm{Tot}(\Gamma_c(V, G(\mathcal{F})) \otimes \Gamma(V, G(\mathcal{G}))) & \longrightarrow & \Gamma_c(V, G(\boldsymbol{G}_m))
\end{array}
$$

where the vertical maps are the natural ones and the horizontal pairings are defined earlier. The top rectangle is commutative because of the definition of the pairing involving cohomology with support in a closed subscheme, taking into account the sign conventions in Proposition A.1 in the Appendix. The bottom one is commutative by definition of the pairing involving compact support cohomology.

Assume now that $\mathcal{F}$ and $\mathcal{G}$ are finite flat group schemes. Then the following maps are continuous: the pairing $H^2_c(V,\mathcal{F}) \times H^1(V,\mathcal{G}) \to H^3_c(V,\boldsymbol{G}_m)$ (see Lemma 4.4), the pairing $H^1(\hat{\mathcal{O}}_v,\mathcal{F}) \times H^2_v(\hat{\mathcal{O}}_v,\mathcal{G}) \to H^3_v(\hat{\mathcal{O}}_v,\boldsymbol{G}_m)$ [Milne 1986, Theorem III.7.1] and the map $\bigoplus_{v\in W} H^1(\hat{\mathcal{O}}_v,\mathcal{F}) \to H^2_c(V,\mathcal{F})$ (see Proposition 3.6).

(2) We now prove the commutativity of the rectangle in the middle. Let

$$\tilde{\Gamma}(U,G(\mathcal{F})) := \mathrm{Cone}\Big(\Gamma(U,G(\mathcal{F})) \to \bigoplus_{v\notin U} \Gamma(\hat{K}_v,G(\mathcal{F})) \oplus \bigoplus_{v\in U\setminus V} \Gamma(\hat{\mathcal{O}}_v,G(\mathcal{F}))\Big)[-1].$$

Then functoriality of the cone gives a commutative diagram (similar to (3), where $I^\bullet(\mathcal{F})$ is replaced by $G(\mathcal{F})$ and by $G(\boldsymbol{G}_m)$) of complexes of abelian groups:

$$\begin{array}{ccccc}
\mathrm{Tot}(\Gamma_c(V,G(\mathcal{F})) & \otimes & \Gamma(V,G(\mathcal{G}))) & \longrightarrow & \Gamma_c(V,G(\boldsymbol{G}_m)) \\
{\scriptstyle q}\uparrow & & \uparrow & & \uparrow{\scriptstyle q} \\
\mathrm{Tot}(\tilde{\Gamma}(U,G(\mathcal{F})) & \otimes & \Gamma(U,G(\mathcal{G}))) & \longrightarrow & \tilde{\Gamma}(U,G(\boldsymbol{G}_m)) \\
\downarrow & & \downarrow{\scriptstyle =} & & \downarrow \\
\mathrm{Tot}(\Gamma_c(U,G(\mathcal{F})) & \otimes & \Gamma(U,G(\mathcal{G}))) & \longrightarrow & \Gamma_c(U,G(\boldsymbol{G}_m))
\end{array}$$

Here the maps denoted by q are quasi-isomorphisms (see Remark 2.7 and the proof of the third point in Proposition 2.1, which uses Lemma 2.4). This diagram gives a commutative diagram in the derived category of abelian groups (where all the maps are either the natural ones or the ones constructed above):

$$\begin{array}{ccccc}
\Gamma_c(V,G(\mathcal{F})) & \otimes^{\boldsymbol{L}} & \Gamma(V,G(\mathcal{G})) & \longrightarrow & \Gamma_c(V,G(\boldsymbol{G}_m)) \\
\downarrow & & \uparrow & & \downarrow \\
\Gamma_c(U,G(\mathcal{F})) & \otimes^{\boldsymbol{L}} & \Gamma(U,G(\mathcal{G})) & \longrightarrow & \Gamma_c(U,G(\boldsymbol{G}_m))
\end{array}$$

Taking cohomology of this diagram gives a commutative diagram of abelian groups:

$$\begin{array}{ccccc}
H^r_c(V,\mathcal{F}) & \times & H^s(V,\mathcal{G}) & \longrightarrow & H^{r+s}_c(V,\boldsymbol{G}_m) \\
\downarrow & & \uparrow & & \downarrow \\
H^r_c(U,\mathcal{F}) & \times & H^s(U,\mathcal{G}) & \longrightarrow & H^{r+s}_c(U,\boldsymbol{G}_m)
\end{array}$$

which implies the required commutativity.

The continuity of the maps in the case where $\mathcal{F}$ and $\mathcal{G}$ are finite flat group schemes is a consequence of Lemma 4.4 and of Lemma 3.3.

(3) We now need to prove the commutativity of the bottom rectangle. By Lemma 4.2, the following diagram commutes in the derived category:

$$\begin{array}{ccc} \Gamma_c(U, G(\mathcal{F})) \otimes^{\boldsymbol{L}} \Gamma(U, G(\mathcal{G})) & \longrightarrow & \Gamma_c(U, G(\boldsymbol{G}_m)) \\ \downarrow \qquad\qquad \uparrow & & \downarrow = \\ \Gamma(U, G(\mathcal{F})) \otimes^{\boldsymbol{L}} \Gamma_c(U, G(\mathcal{G})) & \longrightarrow & \Gamma_c(U, G(\boldsymbol{G}_m)) \end{array}$$

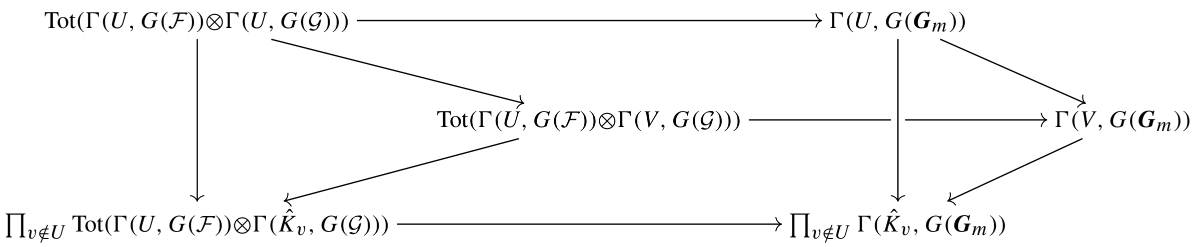
Computing cohomology gives a commutative diagram of abelian groups:

$$\begin{array}{ccc} H^r_c(U, \mathcal{F}) \times H^s(U, \mathcal{G}) & \longrightarrow & H^{r+s}_c(U, \boldsymbol{G}_m) \\ \downarrow \qquad\qquad \uparrow & & \downarrow = \\ H^r(U, \mathcal{F}) \times H^s_c(U, \mathcal{G}) & \longrightarrow & H^{r+s}_c(U, \boldsymbol{G}_m) \end{array}$$

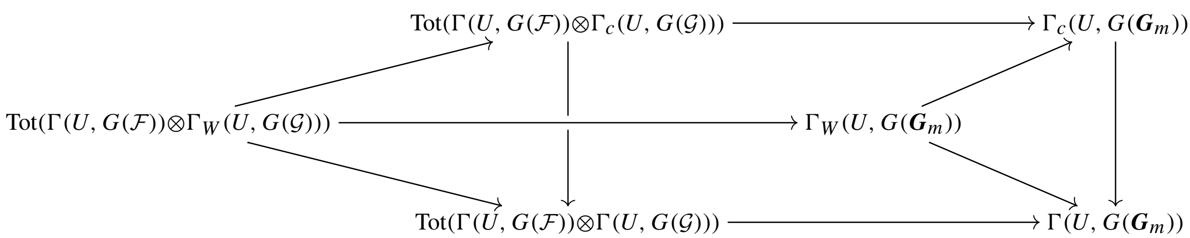
Let $\Gamma_W(U, G(\mathcal{G})) := \mathrm{Cone}(\Gamma(U, G(\mathcal{G})) \to \Gamma(V, G(\mathcal{G})))[-1]$. In order to prove the required commutativity, it is enough to prove that the natural diagram

$$\begin{array}{ccc} \Gamma(U, G(\mathcal{F})) \otimes^{\boldsymbol{L}} \Gamma_c(U, G(\mathcal{G})) & \longrightarrow & \Gamma_c(U, G(\boldsymbol{G}_m)) \\ =\uparrow \qquad\qquad \uparrow & & \uparrow \\ \Gamma(U, G(\mathcal{F})) \otimes^{\boldsymbol{L}} \Gamma_W(U, G(\mathcal{G})) & \longrightarrow & \Gamma_W(U, G(\boldsymbol{G}_m)) \end{array}$$

commutes in the derived category, where the pairing on the bottom row is defined in a similar way as the pairing (10). Consider the following diagram in the category of complexes:



This diagram is commutative, hence, using Proposition A.1, it induces a commutative diagram of complexes at the level of cones:



The commutativity of the upper face of this last diagram concludes the proof.

Assume now that $\mathcal{F}$ and $\mathcal{G}$ are finite flat group schemes. The only possibly nondiscrete groups in the diagram are $H^2_c(U,\mathcal{F})$ (in the case $r=1$) and $H^1(\hat{\mathcal{O}}_v,\mathcal{F})$ (in the case $r=2$). If $r=1$, the pairing $H^2_c(U,\mathcal{F})\times H^1(U,\mathcal{G})\to H^3_c(U,\boldsymbol{G}_m)$ is continuous by Lemma 4.4 and $H^2(\hat{\mathcal{O}}_v,\mathcal{F})=0$ for all $v\in W$ (see for instance [Milne 1986, Lemma 1.1]), hence all maps are continuous in this case. If $r=2$, then the local pairings $H^1(\hat{\mathcal{O}}_v,\mathcal{F})\times H^2_v(\hat{\mathcal{O}}_v,\mathcal{G})\to H^3_v(\hat{\mathcal{O}}_v,\boldsymbol{G}_m)$ are continuous by [Milne 1986, Theorem III.7.1]. All the other maps are obviously continuous.

This finishes the proof of Lemma 4.7. □

We can now prove the following lemma [Milne 1986, Lemma III.8.4]:

Lemma 4.8. *Let $V\subset U$ be a nonempty open subscheme. Let N be a finite flat commutative group scheme over U. Then Theorem 1.1 holds for N over U if and only if it holds for $N_{|V}$ over V.*

Proof. Propositions 2.1(3), 2.12, and 3.6 and Lemma 4.7 give a commutative diagram of long exact sequences of topological groups

$$\begin{array}{ccccccccc}
\cdots \longrightarrow & H^{3-r}_c(V,N) & \longrightarrow & H^{3-r}_c(U,N) & \longrightarrow & \bigoplus_{v\in U\setminus V} H^{3-r}(\hat{\mathcal{O}}_v,N) & \longrightarrow \cdots \\
& \downarrow & & \downarrow & & \downarrow & \\
\cdots \longrightarrow & H^r(V,N^D)^* & \longrightarrow & H^r(U,N^D)^* & \longrightarrow & \bigoplus_{v\in U\setminus V} H^r_v(\hat{\mathcal{O}}_v,N^D)^* & \longrightarrow \cdots
\end{array}$$

where the vertical maps are defined via the pairings (9) and the local duality pairings of [Milne 1986, III.7.1]. In particular, the maps $H^{3-r}(\hat{\mathcal{O}}_v,N)\to H^r_v(\hat{\mathcal{O}}_v,N^D)^*$ are isomorphisms by [Milne 1986, Theorem III.7.1]. The middle vertical map is strict by Lemmas 4.4 and 3.4. Therefore the five-lemma gives the result. □

The end of the proof of Theorem 1.1 (which implies in particular that by duality the groups $H^r(U,N^D)$ are zero for $r\geq 4$, resp. for $r=3$ if $U\neq X$) is exactly the same as the end of the proof of Theorem III.8.2 in [Milne 1986]. Let $U\subset X$ be a nonempty open subset and N be a finite flat commutative group scheme over U:

- If the order of N is prime to p, then Theorem 1.1 is a consequence of Proposition 2.1(4) and étale Artin–Verdier duality (Corollary II.3.3 in [Milne 1986] or Theorem 4.6 in [Geisser and Schmidt 2018]). Note that it requires to compare the pairing defined in Lemma 4.1 with the Artin–Verdier pairing using Ext groups as defined in [Milne 1986] or [Geisser and Schmidt 2018] : this is explained for instance in Proposition A.2 of the Appendix. Hence by Lemma 4.6, it is sufficient to prove Theorem 1.1 when the order of N is a power of p.

- If the order of N is a power of p, the proof of Proposition 3.5 implies that N admits a composition series such that the generic fiber of each quotient is either of height one or the dual of a group of height one. By Lemma 4.6, it is therefore sufficient to prove Theorem 1.1 in the case N_K or N_K^D have height one.

- If N_K or N_K^D have height one, Proposition B.4 and Corollary B.5 in [Milne 1986] imply that there exists a nonempty open subset $V\subset U$ such that $N_{|V}$ extends to a finite flat commutative group scheme $\tilde{N}$

over the proper k-curve X, such that $\tilde{N}$ or $\tilde{N}^D$ have height one. Using Lemma 4.8 twice, it is enough to prove Theorem 1.1 when $U = X$ and N or N^D have height one.

• Lemma III.8.5 in [Milne 1986] proves Theorem 1.1 for $U = X$ and N (resp. N^D) of height one, by reduction to the classical Serre duality for vector bundles over the smooth projective curve X. Indeed, Proposition V.1.20 in [Milne 1980] proves that the pairings $R\Gamma(X, \mathcal{F}^D) \otimes^{\boldsymbol{L}} R\Gamma(X, \mathcal{F}) \to R\Gamma(X, \boldsymbol{G}_m)$ defined via Godement resolutions in the proof of Lemma 4.1 are compatible with the classical pairings using Ext groups that appear in Serre duality.

As observed in [Milne 1986, Section III.8] (remark before Lemma 8.9), the group $H^1(U, N)$ is in general infinite if $U \neq X$ and by duality, the same is true for $H^2_c(U, N)$. However, the situation is better for H^2 and H^1_c.

Corollary 4.9. *Let N be a finite and flat commutative group scheme over a nonempty Zariski open subset U of X. Then the groups $H^2(U, N)$ and $H^1_c(U, N)$ are finite.*

Proof. The statement about $H^1_c(U, N)$ is Corollary 3.2. The finiteness of $H^2(U, N)$ follows by the duality Theorem 1.1. □

The previous corollary can be refined in some cases.

Proposition 4.10. *Let N be a finite and flat commutative group scheme over a nonempty affine open subset $U \subset X$, such that the generic fiber N_K is local. Then $H^1_c(U, N) = 0$.*

Proof. By the valuative criterion of properness, the restriction map $H^1(U, N) \to H^1(K, N)$ is injective. It is sufficient to show that if we choose $v \notin U$, the restriction map $H^1(K, N) \to H^1(\hat{K}_v, N)$ is injective when N_K is local. Indeed this implies that $D^1(U, N) = 0$, hence $H^1_c(U, N) = 0$ by exact sequence (6) because $H^0(\hat{K}_v, N) = 0$ for every completion $\hat{K}_v$ of K.

We also reduce to showing that for every finite subextension L/K of $\hat{K}_v/K$, the restriction map $r : H^1(K, N) \to H^1(L, N)$ is injective (indeed a K-torsor under the finite K-group scheme N_K is of finite type over K, hence it has a point over an extension K' of K if and only if it has a point over a finite subextension of K'). To do this, we argue as in [Česnavičius 2015b, Lemma 5.7(a)]. Since by [Ribenboim 1968, Section F, Theorem 2], L is a separable extension of K, the K-algebra $E := L \otimes_K L$ is reduced. As N_K is finite and connected, the group $N(E)$ is trivial. Let $C^1 := \boldsymbol{R}_{E/K}(N \times_K E)$ (where $\boldsymbol{R}$ denotes Weil's restriction of scalars) be the scheme of 1-cochains with respect to L/K, we obtain that $C^1(K)$ is trivial, which in turn implies that $\ker r$ is trivial by [Česnavičius 2015b, Section 5.1]. □

Remark 4.11. The finiteness of $H^1_c(U, N)$ (Corollary 3.2) relies on the finiteness of $D^1(U, N)$ proven in [Česnavičius 2017, Theorem 2.9]. An alternative argument is actually available. By [Milne 1986, Lemma III.8.9], we can assume that $U \neq X$, namely that U is affine. By [loc. cit., Theorem II.3.1] and Proposition 2.1(4), we can also assume that the order of N is a power of p. Let N_K be the generic fiber of N, it is a finite group scheme over K. By [Demazure and Gabriel 1970, IV, Section3.5], and Proposition 2.1(2), it is sufficient to prove the required finiteness in the following cases: N_K is étale, N_K is local with étale dual, $N_K = \alpha_p$. The last two cases are taken care of by Proposition 4.10, so we can suppose that N_K is étale. Let $V \subset U$ be a nonempty open subset. By Proposition 2.1, we have an exact sequence

$$H^1_c(V, N) \to H^1_c(U, N) \to \bigoplus_{v \in U \setminus V} H^1(\hat{\mathcal{O}}_v, N).$$

Since the generic fiber of N is étale, the group $H^1(\hat{\mathcal{O}}_v, N)$ is finite by [Milne 1986, Remark III.7.6] (this follows from the fact that $H^1(\hat{\mathcal{O}}_v, N)$ is a compact subgroup of the discrete group $H^1(K_v, N)$), hence the finiteness of $H^1_c(U, N)$ is equivalent to the finiteness of $H^1_c(V, N)$, which in turn is equivalent to the finiteness of $D^1(V, N)$. The latter holds for V sufficiently small: either apply [González-Avilés 2009, Lemma 4.3] (which relies on an embedding of N_K into an abelian variety) or reduce (as in [Milne 1986, Lemma III.8.9]) to the case when N^D is of height one. Indeed by [loc. cit., Corollary III.B.5], the assumption that N^D is of height one implies that for V sufficiently small, the restriction of N to V extends to a finite and flat commutative group scheme $\tilde{N}$ over X. Then the finiteness of $H^1_c(X, \tilde{N})$ implies the finiteness of $H^1_c(V, \tilde{N}) = H^1_c(V, N)$ by Proposition 2.1(3), because the groups $H^0(\hat{\mathcal{O}}_v, \tilde{N})$ are finite.

5. The number field case

Assume now that K is a number field and set $X = \operatorname{Spec} \mathcal{O}_K$. Let U be a nonempty Zariski open subset of X. Let n be the order of the finite and flat commutative group scheme N. To prove Theorem 1.1 in this case, one follows exactly the same method as in [Milne 1986, Theorem III.3.1 and Corollary III.3.2], once Proposition 2.1 has been proved. Namely Proposition 2.1(4) shows that on $U[1/n]$, Theorem 1.1 reduces to the étale Artin–Verdier Theorem [Milne 1986, II.3.3] or [Geisser and Schmidt 2018, Theorem 4.6]. Here we can use a definition of the pairings similar to Lemma 4.1, or a definition via the Ext pairings as in [loc. cit.] (the two definitions coincide, the argument being the same as in Proposition A.2 of the Appendix). Now Proposition 2.1(3) gives a commutative diagram as in the end of the proof of [Milne 1986, Theorem III.3.1] (with completions $\hat{\mathcal{O}}_v$ instead of henselizations $\mathcal{O}_v$). Theorem 1.1 follows by the five-lemma, using the result on $U[1/n]$ and the local duality statement [Milne 1986, Theorem III.3.1].

Remark 5.1. In the number field case, one can as well (as in [Milne 1986, Section III.3]) work from the very beginning with henselizations $\mathcal{O}_v$ and not with completions $\hat{\mathcal{O}}_v$ to define cohomology with compact support. Indeed the local theorem [loc. cit., Theorem III.3.1] still holds with henselian (not necessarily complete) discrete valuation ring with finite residue field when the fraction field is of characteristic zero. Hence the only issue here is commutativity of diagrams. Nevertheless, we felt that it was more convenient to have a uniform statement (Proposition 2.1) in both characteristic 0 and characteristic p situations.

Appendix

A.1. *Cone and tensor products.*

Proposition A.1. *Let $\mathcal{A}$ be the category of fppf sheaves over a scheme T. Let A, B and C be three complexes in $\mathcal{A}$. Let $f : A \to B$ be a morphism of complexes. Then there are commutative diagrams* (*where* $\otimes$ *denotes the total tensor product of complexes*) *such that the vertical maps are isomorphisms of complexes*

$$\begin{array}{ccccccc} A\otimes C & \xrightarrow{f\otimes 1} & B\otimes C & \xrightarrow{i\otimes 1} & \mathrm{Cone}(f)\otimes C & \xrightarrow{-\pi\otimes 1} & A[1]\otimes C \\ \downarrow{=} & & \downarrow{=} & & \downarrow{\sim} & & \downarrow{\sim} \\ A\otimes C & \xrightarrow{f\otimes 1} & B\otimes C & \xrightarrow{i'} & \mathrm{Cone}(f\otimes 1) & \xrightarrow{-\pi} & (A\otimes C)[1] \end{array}$$

where the vertical isomorphisms involve no signs, *and*

$$\begin{array}{ccccccc} C\otimes A & \xrightarrow{1\otimes f} & C\otimes B & \xrightarrow{1\otimes i} & C\otimes \mathrm{Cone}(f) & \xrightarrow{-1\otimes\pi} & C\otimes A[1] \\ \downarrow{=} & & \downarrow{=} & & \downarrow{\sim} & & \downarrow{\sim} \\ C\otimes A & \xrightarrow{1\otimes f} & C\otimes B & \xrightarrow{i'} & \mathrm{Cone}(1\otimes f) & \xrightarrow{-\pi} & (C\otimes A)[1] \end{array}$$

where the two last vertical maps involve a sign $(-1)^r$ *on the factor* $C_r\otimes A_s$.

Proof. In the first diagram, define the nonobvious map $\mathrm{Cone}(f)\otimes C\to\mathrm{Cone}(f\otimes 1)$ (resp. $A[1]\otimes C\to(A\otimes C)[1]$) by the isomorphism $(B_r\oplus A_{r+1})\otimes C_s\to(B_r\otimes C_s)\oplus(A_{r+1}\otimes C_s)$ (resp. by the identity of $A_{r+1}\otimes C_s$). In the second diagram, the nonobvious map $C\otimes\mathrm{Cone}(f)\to\mathrm{Cone}(1\otimes f)$ (resp. $C\otimes A[1]\to(C\otimes A)[1]$) is given by the isomorphism $C_r\otimes(B_s\oplus A_{s+1})\to(C_r\otimes B_s)\oplus(C_r\otimes A_{s+1})$ that maps $c\otimes(b,a)$ to $(c\otimes b,(-1)^r c\otimes a)$ (resp. by the automorphism of $C_r\otimes A_{s+1}$ given by $c\otimes a\mapsto(-1)^r c\otimes a$). The proposition is then straightforward. □

A.2. ***Comparison of two pairings.*** Let U be a nonempty Zariski open subset of a smooth, projective, geometrically integral curve defined over a finite field.

Proposition A.2. *Let* A, B *and* C *be three fppf sheaves on* U, *endowed with a pairing* $A\otimes B\to C$. *Then there is a commutative diagram*

$$\begin{array}{ccc} H^r(U,A)\otimes H^s_c(U,B) & \longrightarrow & H^{r+s}_c(U,C) \\ \downarrow & & \downarrow{=} \\ \mathrm{Ext}^r_U(B,C)\otimes H^s_c(U,B) & \longrightarrow & H^{r+s}_c(U,C) \end{array}$$

where the top pairing is the one from (10) *and the bottom one is the pairing from* [Milne 1986, Proposition III.0.4.e]. *The same holds for étale sheaves instead of fppf sheaves if we replace fppf cohomology* (*resp. compact support fppf cohomology*) *by étale cohomology* (*resp. compact support étale cohomology*); *in the étale case the bottom pairing is the one from* [loc. cit., Proposition II.2.5] (*or* [Geisser and Schmidt 2018]).

Proof. We prove the statement for fppf sheaves (the étale case is similar). Consider the natural morphisms of complexes

$$\mathrm{Tot}(G(A)\otimes G(B)) \to G(A\otimes B) \to G(C).$$

Using [Stacks 2005–, Tag 0A90], one gets a natural morphism of complexes $G(A)\to \mathcal{H}om^\bullet(G(B), G(C))$ and a commutative diagram of complexes

$$\begin{array}{ccc}
\mathrm{Tot}(G(A)\otimes G(B)) \longrightarrow G(A\otimes B) & \longrightarrow & G(C) \\
\downarrow & & \downarrow = \\
\mathrm{Tot}(\mathcal{H}om^\bullet(G(B), G(C))\otimes G(B)) & \longrightarrow & G(C)
\end{array}$$

where the second pairing is the natural one. All morphisms in this diagram involve no extra-sign.

Let $G(C)\to I$ be an injective resolution. Then one gets a commutative diagram:

$$\begin{array}{ccc}
\mathrm{Tot}(G(A)\otimes G(B)) \longrightarrow G(A\otimes B) & \longrightarrow & G(C) \\
\downarrow & & \downarrow \\
\mathrm{Tot}(\mathcal{H}om^\bullet(G(B), I)\otimes G(B)) & \longrightarrow & I
\end{array}$$

Taking global sections, one gets a commutative diagram:

$$\begin{array}{ccc}
\mathrm{Tot}(\Gamma(U, G(A))\otimes \Gamma(U, G(B))) & \longrightarrow & \Gamma(U, G(C)) \\
\downarrow & & \downarrow \sim \\
\mathrm{Tot}(\mathrm{Hom}^\bullet_U(G(B), I)\otimes \Gamma(U, G(B))) & \longrightarrow & \Gamma(U, I)
\end{array} \tag{1}$$

Taking cohomology, one gets a commutative diagram comparing the pairing from the beginning of Section 4 to the classical Ext-pairing:

$$\begin{array}{ccc}
H^r(U, A)\otimes H^s(U, B) & \longrightarrow & H^{r+s}(U, C) \\
\downarrow & & \downarrow = \\
\mathrm{Ext}^r_U(B, C)\otimes H^s(U, B) & \longrightarrow & H^{r+s}(U, C)
\end{array}$$

Applying functoriality of cone to (1) and to the similar pairing over completions of K, one gets a commutative diagram of complexes:

$$\begin{array}{ccc}
\mathrm{Tot}(\Gamma(U, G(A))\otimes \Gamma_c(U, G(B))) & \longrightarrow & \Gamma_c(U, G(C)) \\
\downarrow & & \downarrow \sim \\
\mathrm{Tot}(\mathrm{Hom}^\bullet_U(G(B), I)\otimes \Gamma_c(U, G(B))) & \longrightarrow & \Gamma_c(U, I)
\end{array}$$

Taking cohomology, we get the required commutative diagram. □

Remarks A.3. (1) A similar diagram holds with compact support cohomology groups on the left and Ext-groups on the right. In this case, one gets a commutative diagram:

$$\begin{array}{ccc} H^r_c(U,A)\otimes H^s(U,B) & \longrightarrow & H^{r+s}_c(U,C) \\ \downarrow & & \downarrow = \\ H^r_c(U,A)\otimes \mathrm{Ext}^s_U(A,C) & \longrightarrow & H^{r+s}_c(U,C) \end{array}$$

where the first pairing is the one from Lemma 4.1, while the vertical map and the bottom pairing both involve a $(-1)^{rs}$ sign.

(2) Similar commutative diagrams hold over an arbitrary basis, with compact support cohomology replaced by cohomology with support in a closed subscheme (with a similar proof).

Acknowledgments

We thank K. Česnavičius, C. Pépin, A. Schmidt and T. Szamuely for enlightening comments on the first draft of this paper. We also thank T. Suzuki for sharing his preprint [Suzuki 2018]. We warmly thank the anonymous referee for his/her very thorough reading of the article and for having made numerous interesting suggestions.

References

[Artin 1969] M. Artin, "Algebraic approximation of structures over complete local rings", *Inst. Hautes Études Sci. Publ. Math.* **36** (1969), 23–58. MR Zbl

[Artin and Milne 1976] M. Artin and J. S. Milne, "Duality in the flat cohomology of curves", *Invent. Math.* **35** (1976), 111–129. MR Zbl

[Bauer 1992] W. Bauer, "On the conjecture of Birch and Swinnerton-Dyer for abelian varieties over function fields in characteristic $p > 0$", *Invent. Math.* **108**:2 (1992), 263–287. MR Zbl

[Beilinson et al. 1982] A. A. Beilinson, J. Bernstein, and P. Deligne, "Faisceaux pervers", pp. 5–171 in *Analysis and topology on singular spaces, I* (Luminy, France, 1981), Astérisque **100**, Soc. Math. France, Paris, 1982. MR Zbl

[Bourbaki 2006] N. Bourbaki, *Algèbre commutative, Chapitres V–VII*, chapter VI, Springer, 2006. Definitive edition (chapters V–VII) published by Hermann, Paris, 1964; translated as *Commutative algebra*, Addison-Wesley, Reading, MA, 1972.

[Bourbaki 2007] N. Bourbaki, *Topologie générale, Chapitres I–IV*, chapter III, Springer, 2007. Definitive edition (chapters I–IV) published by Hermann, Paris, 1960; translated as *General topology*, Springer, 1971.

[Česnavičius 2015a] K. Česnavičius, "Poitou–Tate without restrictions on the order", *Math. Res. Lett.* **22**:6 (2015), 1621–1666. MR Zbl

[Česnavičius 2015b] K. Česnavičius, "Topology on cohomology of local fields", *Forum Math. Sigma* **3** (2015), art. id. e16. MR Zbl

[Česnavičius 2017] K. Česnavičius, "p-Selmer growth in extensions of degree p", *J. Lond. Math. Soc.* (2) **95**:3 (2017), 833–852. MR Zbl

[Demarche 2011a] C. Demarche, "Le défaut d'approximation forte dans les groupes linéaires connexes", *Proc. Lond. Math. Soc.* (3) **102**:3 (2011), 563–597. MR Zbl

[Demarche 2011b] C. Demarche, "Suites de Poitou–Tate pour les complexes de tores à deux termes", *Int. Math. Res. Not.* **2011**:1 (2011), 135–174. MR Zbl

[Demazure and Gabriel 1970] M. Demazure and P. Gabriel, *Groupes algébriques, I: Géométrie algébrique, généralités, groupes commutatifs*, Masson & Cie, Paris, 1970. MR Zbl

[EGA IV_4 1967] A. Grothendieck, "Eléments de géométrie algébrique, IV: Étude locale des schémas et des morphismes de schémas, IV", *Inst. Hautes Études Sci. Publ. Math.* **32** (1967), 5–361. MR Zbl

[Friedlander and Suslin 2002] E. M. Friedlander and A. Suslin, "The spectral sequence relating algebraic K-theory to motivic cohomology", *Ann. Sci. École Norm. Sup.* (4) **35**:6 (2002), 773–875. MR Zbl

[Gabber and Kelly 2015] O. Gabber and S. Kelly, "Points in algebraic geometry", *J. Pure Appl. Algebra* **219**:10 (2015), 4667–4680. MR Zbl

[Gabber et al. 2014] O. Gabber, P. Gille, and L. Moret-Bailly, "Fibrés principaux sur les corps valués henséliens", *Algebr. Geom.* **1**:5 (2014), 573–612. MR Zbl

[Geisser and Schmidt 2018] T. H. Geisser and A. Schmidt, "Poitou–Tate duality for arithmetic schemes", *Compos. Math.* **154**:9 (2018), 2020–2044. MR Zbl

[Gille and Pianzola 2008] P. Gille and A. Pianzola, "Isotriviality and étale cohomology of Laurent polynomial rings", *J. Pure Appl. Algebra* **212**:4 (2008), 780–800. MR Zbl

[Godement 1958] R. Godement, *Topologie algébrique et théorie des faisceaux*, Actual. Sci. Ind. **1252**, Hermann, Paris, 1958. MR Zbl

[González-Avilés 2009] C. D. González-Avilés, "Arithmetic duality theorems for 1-motives over function fields", *J. Reine Angew. Math.* **632** (2009), 203–231. MR Zbl

[Grothendieck 1968] A. Grothendieck, "Le groupe de Brauer, III: Exemples et compléments", pp. 88–188 in *Dix exposés sur la cohomologie des schémas*, Adv. Stud. Pure Math. **3**, North-Holland, Amsterdam, 1968. MR Zbl

[Harari and Szamuely 2005] D. Harari and T. Szamuely, "Arithmetic duality theorems for 1-motives", *J. Reine Angew. Math.* **578** (2005), 93–128. MR Zbl

[Kashiwara and Schapira 2006] M. Kashiwara and P. Schapira, *Categories and sheaves*, Grundlehren der Math. Wissenschaften **332**, Springer, 2006. MR Zbl

[Kato and Trihan 2003] K. Kato and F. Trihan, "On the conjectures of Birch and Swinnerton-Dyer in characteristic $p > 0$", *Invent. Math.* **153**:3 (2003), 537–592. MR Zbl

[Matsumura 1970] H. Matsumura, *Commutative algebra*, Benjamin, New York, 1970. MR Zbl

[Mazur 1972] B. Mazur, "Rational points of abelian varieties with values in towers of number fields", *Invent. Math.* **18** (1972), 183–266. MR Zbl

[Milne 1980] J. S. Milne, *Étale cohomology*, Princeton Math. Series **33**, Princeton Univ. Press, 1980. MR Zbl

[Milne 1986] J. S. Milne, *Arithmetic duality theorems*, Perspect. Math. **1**, Academic Press, Boston, 1986. MR Zbl

[Moret-Bailly 2012] L. Moret-Bailly, "An extension of Greenberg's theorem to general valuation rings", *Manuscripta Math.* **139**:1-2 (2012), 153–166. MR Zbl

[Peters and Steenbrink 2008] C. A. M. Peters and J. H. M. Steenbrink, *Mixed Hodge structures*, Ergebnisse der Mathematik (3) **52**, Springer, 2008. MR Zbl

[Ribenboim 1968] P. Ribenboim, *Théorie des valuations*, Sémin. Math. **9**, Univ. Montreal, 1968. MR Zbl

[Rosengarten 2018] Z. Rosengarten, "Tate duality in positive dimension over function fields", preprint, 2018. arXiv

[SGA 4_1 1972] M. Artin, A. Grothendieck, and J. L. Verdier, *Théorie des topos et cohomologie étale des schémas, Tome 1: Théorie des topos, Exposés I–IV* (Séminaire de Géométrie Algébrique du Bois Marie 1963–1964), Lecture Notes in Math. **269**, Springer, 1972. MR Zbl

[SGA 4_2 1972] M. Artin, A. Grothendieck, and J. L. Verdier, *Théorie des topos et cohomologie étale des schémas, Tome 2: Exposés V–VIII* (Séminaire de Géométrie Algébrique du Bois Marie 1963–1964), Lecture Notes in Math. **270**, Springer, 1972. MR Zbl

[SGA 4_3 1973] M. Artin, A. Grothendieck, and J. L. Verdier, *Théorie des topos et cohomologie étale des schémas, Tome 3: Exposés IX–XIX* (Séminaire de Géométrie Algébrique du Bois Marie 1963–1964), Lecture Notes in Math. **305**, Springer, 1973. MR Zbl

[Stacks 2005–] P. Belmans, A. J. de Jong, et al., "The Stacks project", electronic reference, 2005–, Available at http://stacks.math.columbia.edu.

[Suzuki 2018] T. Suzuki, "Duality for cohomology of curves with coefficients in abelian varieties", *Nagoya Math. J.* (online publication December 2018).

[Toën 2011] B. Toën, "Descente fidèlement plate pour les n-champs d'Artin", *Compos. Math.* **147**:5 (2011), 1382–1412. MR Zbl

Communicated by Bjorn Poonen
Received 2018-05-01 Revised 2019-07-03 Accepted 2019-08-01

cyril.demarche@imj-prg.fr *Institut de Mathématiques de Jussieu-Paris Rive Gauche, Sorbonne Université, Paris, France*

david.harari@math.u-psud.fr *Laboratoire de Mathématiques d'Orsay, Université Paris-Sud, Orsay, France*

ALGEBRA AND NUMBER THEORY 13:10 (2019)
dx.doi.org/10.2140/ant.2019.13.2359

Betti numbers of Shimura curves and arithmetic three-orbifolds

Mikołaj Frączyk and Jean Raimbault

We show that asymptotically the first Betti number b_1 of a Shimura curve satisfies the Gauss–Bonnet equality $2\pi(b_1-2)=\mathrm{vol}$ where vol is hyperbolic volume; equivalently $2g-2=(1+o(1))\mathrm{vol}$ where g is the arithmetic genus. We also show that the first Betti number of a congruence hyperbolic 3-orbifold asymptotically vanishes relatively to hyperbolic volume, that is $b_1/\mathrm{vol}\to 0$. This generalizes previous results obtained by Frączyk, on which we rely, and uses the same main tool, namely Benjamini–Schramm convergence.

1. Introduction

1A. ***Benjamini–Schramm convergence.*** Let G be a semisimple Lie group, $K\subset G$ a maximal compact subgroup and $X=G/K$ the associated symmetric space. Benjamini–Schramm convergence of locally symmetric orbifolds $\Gamma\backslash X$ of finite volume was introduced in [Abert et al. 2017]. The Benjamini–Schramm convergence of a sequence of finite volume locally symmetric spaces $(\Gamma_i\backslash X)_{i\in\mathbb{N}}$ to the symmetric space X is equivalent to the following simple geometric condition:

$$\forall R>0,\ \lim_{i\to\infty}\frac{\mathrm{vol}((\Gamma_i\backslash X)_{<R})}{\mathrm{vol}(\Gamma_i\backslash X)}=0, \tag{1-1}$$

where $M_{<R}$ denotes the R-thin part of a Riemannian orbifold M (which we take to include the full singular set, see (3-1) below).

In addition to X there are other possible limits in the Benjamini–Schramm topology. In order to describe them it is convenient to pass to the language of invariant random subgroups (IRS) of the group G. These are the Borel probability measures on the Chabauty space Sub_G of closed subgroups which are invariant under conjugation by elements of G. For every lattice Γ of G there is a unique G-invariant probability measure on G/Γ and its pushforward by the map $g\Gamma\mapsto g\Gamma g^{-1}$ gives an IRS denoted μ_Γ. It was observed in [Abert et al. 2017] that $(\Gamma_i\backslash X)$ converges to X if and only if μ_{Γ_i} converge weakly-* to the trivial IRS $\delta_{\{1\}}$. In general a sequence $(\Gamma_i\backslash X)$ converges Benjamini–Schramm if and only if μ_Γ

The writing of this paper was facilitated by a visit of the second author to the Rényi Institute, funded by ERC Consolidator Grant 648017 to Miklós Abért. The second author also benefited from support from the grant ANR-16-CE40-0022-01 - AGIRA. The first author was supported by ERC Consolidator Grant 648017. We are grateful to an anonymous referee who pointed out a gap in a previous version of this paper.
MSC2010: primary 11F06; secondary 20H10.
Keywords: Shimura curves, arithmetic hyperbolic manifolds, Betti numbers.

converges weakly-* to some IRS ν. The limit IRS ν is always supported on discrete subgroups and the Benjamini–Schramm limit is the random locally symmetric space X/Λ where Λ is a ν-random subgroup of G.

It was proven in [Abert et al. 2017], as a consequence of the Nevo–Stück–Zimmer theorem, that if G is semisimple of higher rank, with all factors having property (T) then any sequence of irreducible locally symmetric spaces converges in the Benjamini–Schramm sense to X. This was extended to all nontrivial products in [Levit 2017] (see also [Matz 2019] for more precise results in a very specific case).

This statement is known to be false when $G = \mathrm{SO}(n, 1)$ or $\mathrm{SU}(n, 1)$, because in those cases there are lattices $\Gamma \subset G$ such that $H^1(\Gamma, \mathbb{R}) \neq 0$ (see [Millson 1976; Li and Millson 1993; Kazhdan 1977]). On the other hand restricting attention to the family of *arithmetic congruence lattices* in G (see Section 1D below for a short description) Fraczyk [2016] proved that for $G = \mathrm{SO}(2, 1)$ or $\mathrm{SO}(3, 1)$ the symmetric space $X = \mathbb{H}^2$ or $\mathbb{H}^3$, respectively, is the only possible limit in the Benjamini–Schramm topology for a sequence of torsion-free congruence lattices. Previously Raimbault [2017] proved a similar result for the family of nonuniform, not necessarily torsion-free lattices (nonuniformity makes them much easier to deal with algebraically). In this paper we remove the torsion-free hypothesis in general.

Theorem A. If $G = \mathrm{PGL}_2(\mathbb{R})$ or $\mathrm{PGL}_2(\mathbb{C})$ and Γ_n is a sequence of irreducible arithmetic lattices in G, which are either all congruence and pairwise distinct, or pairwise noncommensurable, then the sequence of locally symmetric spaces $\Gamma_n \backslash X$ converges in the Benjamini–Schramm sense to X.

In [Fraczyk 2016] the torsion free assumption was necessary because the methods only allowed control of the volume of the subset of thin part consisting of the collars of short geodesics. For a sequence of general arithmetic congruence orbifolds $(\Gamma_n \backslash X)_{n\in\mathbb{N}}$ it could *a priori* happen that the vast majority of the thin part comes from the cusps or the conical singularities so the sequence does not converge to X. Theorem A excludes this possibility. For the proof we use the estimates developed in [Fraczyk 2016] to show that any weak-* limit of the sequence μ_{Γ_n} is supported on elementary subgroups. By [Osin 2017] the only IRS supported on this set is the trivial IRS, hence the theorem. We carry out the second step of this scheme of proof in detail in Proposition A.4, which is valid for all sequences of lattices in proper Gromov-hyperbolic spaces.

We note that because we are using a soft method our approach does not indicate the rate of decay of $\mathrm{vol}(\Gamma_n \backslash X)_{<R}) / \mathrm{vol}(\Gamma_n \backslash X)$ as opposed to [Fraczyk 2016].

1B. ***Genus of Shimura curves.*** One application of Theorem A is to determine the asymptotic genus of congruence surfaces of large volume. For compact surfaces without singularities the genus and volume are essentially linearly related by the Gauss–Bonnet formula. However for 2-orbifolds terms coming from cone points and cusps appear in the formula, and it is easy to see that there exists sequences of hyperbolic orbifolds with underlying space a sphere and volume going to infinity. This also has an algebraic interpretation: if S is isomorphic as a Riemann surface to the $\mathbb{C}$-points of an algebraic variety defined over a number field, which is the case for orbifolds obtained from congruence groups (so-called Shimura curves [1971]), then its arithmetic genus is given by the Riemann–Hurwitz formula and essentially proportional to the volume while its geometric genus equals the topological genus of the underlying surface and can be arbitrarily smaller than the former.

It is known that this phenomenon cannot occur for congruence orbifolds: using the uniform spectral gap for congruence quotients (see [Clozel 2003] for a more general result) and a theorem of P. Zograf [1991] it follows that there is a lower bound of the form $g \geq c\,\mathrm{vol}$ for congruence subgroups (see also [Long et al. 2006]). As a consequence of Theorem A we obtain the following asymptotically more precise result (we note that it was known for congruence covers of the modular surface by a result of J. G. Thompson [1980]).

Theorem B. Let Γ_n be a sequence of congruence lattices in $\mathrm{PSL}_2(\mathbb{R})$, and let g_n be the topological genus of the orbifold $O_n = \Gamma_n \backslash \mathbb{H}^2$. Then, assuming the Γ_n are not pairwise conjugated, we have

$$\lim_{n\to+\infty} \frac{g_n}{\mathrm{vol}\, O_n} = \frac{1}{4\pi}.$$

1C. *Betti numbers of 3-orbifolds.* Theorem B is equivalent to the statement that $b_1(\Gamma_n)/\,\mathrm{vol}(\Gamma_n\backslash\mathbb{H}^2)$ converges to $1/2\pi$ for a sequence of congruence lattices. Indeed, the rank of abelianization is essentially equal to twice the genus in a BS-convergent sequence. This can be proven more directly by analytical means, as $1/2\pi$ is the first L^2-Betti number of the hyperbolic plane. While more complicated, the analytic approach generalizes to the dimension 3 and where obtain the following result.

Theorem C. Let Γ_n be a sequence of congruence lattices in $\mathrm{PSL}_2(\mathbb{C})$. Then

$$\lim_{n\to+\infty} \frac{b_1(\Gamma_n)}{\mathrm{vol}(\Gamma_n\backslash\mathbb{H}^3)} = 0.$$

This was proven in [Raimbault 2017] for nonuniform lattices, and in [Fraczyk 2016] for the case of all torsion-free lattices. Our proof is very similar to the proof for hyperbolic 3–manifolds appearing in [Abert et al. 2017].

1D. *Congruence lattices.* For completeness we give an explicit description of the congruence arithmetic latices in $G = \mathrm{PGL}(2, \mathbb{R}), \mathrm{PGL}(2, \mathbb{C})$, though we will not directly use this structure theory in the rest of the paper. Let $\mathbb{K} = \mathbb{R}, \mathbb{C}$. We start by choosing a number field k with Archimedean places $\nu_1, \ldots, \nu_d$ such that $k_{\nu_1} \simeq \mathbb{K}$ and $k_{\nu_i} \simeq \mathbb{R}$ for $i \geq 2$. In what follows $\mathbb{A}$ and $\mathbb{A}_f$ stand for the ring of adèles and, respectively, finite adèles of k. We will write $k \ni x \mapsto (x)_\nu \in k_\nu$ for the embedding of k in its completion k_ν. Let $a, b \in k^\times$ be such that $(a)_{\nu_i}, (b)_{\nu_i}$ are positive for $i \geq 2$ and $(a)_{\nu_1}$ or $(b)_{\nu_1}$ is negative if $\mathbb{K} \simeq \mathbb{R}$. We define the quaternion algebra A as

$$A = k + \boldsymbol{i}k + \boldsymbol{j}k + \boldsymbol{ij}k,$$

subject to the relations $\boldsymbol{i}^2 = -a$, $\boldsymbol{j}^2 = -b$, $\boldsymbol{ij} = -\boldsymbol{ji}$. By our choice of a, b we have $A \otimes_k k_{\nu_1} \simeq M(2, \mathbb{K})$ and for $i \geq 2$ the algebra $A \otimes_k k_{\nu_i}$ is isomorphic to the Hamilton's quaternions. We form an algebraic group $\mathrm{PA}^\times = A^\times/k^\times$. It is an adjoint simple group of type A_1 defined over k. Note that $\mathrm{PA}^\times(\mathbb{A}) =$

$\mathrm{PA}^\times(k \otimes_{\mathbb{Q}} \mathbb{R}) \times \mathrm{PA}^\times(\mathbb{A}_f)$ and

$$\mathrm{PA}^\times(k \otimes_{\mathbb{Q}} \mathbb{R}) = \prod_{i=1}^{d} \mathrm{PA}^\times(k_{v_i}) \simeq \mathrm{PGL}(2, \mathbb{K}) \times \mathrm{PO}(3)^{d-1}.$$

Choose an open compact subgroup U of $\mathrm{PA}^\times(\mathbb{A}_f)$. Let $\Gamma_U = \mathrm{PA}^\times(k) \cap (\mathrm{PA}^\times(k \otimes_{\mathbb{Q}} \mathbb{R}) \times \mathrm{PA}^\times(\mathbb{A}_f))$. By a classical result of Borel and Harish-Chandra [1962] the group Γ_U is a lattice in $\mathrm{PA}^\times(k \otimes_{\mathbb{Q}} \mathbb{R}) \times \mathrm{PA}^\times(\mathbb{A}_f) \simeq \mathrm{PGL}(2, \mathbb{K}) \times \mathrm{PO}(3)^{d-1} \times U$. The projection of Γ_U to the factor $\mathrm{PGL}(2, \mathbb{K})$ is a *congruence arithmetic lattice* in $\mathrm{PGL}(2, \mathbb{K})$. Every congruence arithmetic lattice of $\mathrm{PGL}(2, \mathbb{K})$ arises in this way.

1E. *Outline of the paper.* In Section 2 we apply a "soft" criterion for Benjamini–Schramm convergence, together with the estimates from [Fraczyk 2016], to deduce Theorem A. The criterion is proven, in a general form including lattices in the isometry group of any proper Gromov-hyperbolic space, in Appendix A Next, in Section 3 we give a precise metric description of the singular locus of hyperbolic 2- and 3-orbifolds, and (in the 3-dimensional case) a way to smooth the boundary of the thick part while keeping control of the geometry (the technical details of which are left to a second Appendix B). We use this description of singularities and Theorem A to deduce Theorem B in Section 4. In Section 5 we use heat kernel methods (for which we need the precise description of the smoothed thick part) to deduce Theorem C from Theorem A.

2. Benjamini–Schramm convergence of quotients of hyperbolic spaces

2A. *A criterion for convergence.* Let G be a semisimple Lie group and γ a semisimple element of G. Let G_γ be the centralizer in G of Γ, then for any sufficiently decreasing (for example compactly supported) continuous function on G the following integral makes sense.

$$\mathcal{O}_f(\gamma) = \int_{G/G_\gamma} f(\gamma^{-1} x \gamma)\, dx \tag{2-1}$$

The following proposition is a generalization of [Raimbault 2017, Proposition 2.2]. We provide a self-contained proof (along the same lines as that of [loc. cit.]) of a much more general result valid for all Gromov-hyperbolic spaces in Proposition A.4 below.

Proposition 2.1. *Let Γ_n be a sequence of lattices in either* $\mathrm{PGL}_2(\mathbb{R})$ *or* $\mathrm{PGL}_2(\mathbb{C})$ *and $d = 2, 3$ accordingly. Let U be the subset of loxodromic elements in G. If for every smooth compactly supported function f on G the limit*

$$\lim_{n\to+\infty} \frac{\sum_{[\gamma]_{\Gamma_n} \subset U} \mathrm{vol}((\Gamma_n)_\gamma \backslash G_\gamma) \mathcal{O}_f(\gamma)}{\mathrm{vol}(\Gamma_n \backslash G)} = 0 \tag{2-2}$$

holds, then $\Gamma_n \backslash \mathbb{H}^d$ is BS-convergent to $\mathbb{H}^d$.

This is essentially tautological if the Γ_n are torsion-free; the nontrivial part is that it allows us to avoid studying the elliptic conjugacy classes (and the parabolic classes if the Γ_n are noncompact) in order to establish BS-convergence of a sequence of orbifolds.

2B. *Proof of Theorem A*. If X is a rank-one irreducible symmetric space such as $\mathbb{H}^2$ or $\mathbb{H}^3$ and $G = \mathrm{Isom}(X)$ then G is a simple Lie group of noncompact type and its elliptic radical is trivial. Theorem A thus follows immediately from Proposition 2.1 and the following result extracted from [Fraczyk 2016].

Theorem 2.2. *Let $G = \mathrm{PGL}_2(\mathbb{R})$ or $\mathrm{PGL}_2(\mathbb{C})$ and let U be the set of hyperbolic elements of G. Let Γ_n a sequence of arithmetic congruence lattices in G, such that $\mathrm{vol}(\Gamma_n\backslash G) \to +\infty$ or any sequence of pairwise noncommensurable arithmetic lattices. Then for any $f \in C_0^\infty(G)$ we have*

$$\frac{1}{\mathrm{vol}(\Gamma_n\backslash G)}\left|\sum_{[\gamma]\subset U} \mathrm{vol}((\Gamma_n)_\gamma\backslash G_\gamma)\mathcal{O}_f(\gamma)\right| \xrightarrow{n\to+\infty} 0. \tag{2-3}$$

Proof. If Γ is an arithmetic lattice in $\mathrm{PGL}_2(\mathbb{R})$ or $\mathrm{PGL}_2(\mathbb{C})$ then an element $\gamma \in \Gamma$ is hyperbolic if and only if it is semisimple and of infinite order. In the proof of [Fraczyk 2016, Theorem 1.8], starting form the lines (10.7–10.9) the author bounds the sum

$$\sum_{\substack{[\gamma]_\Gamma \\ \text{nontorsion}}} \mathrm{vol}(\Gamma_\gamma\backslash G_\gamma)\mathcal{O}_\gamma(f) \tag{2-4}$$

for congruence arithmetic lattices. The line (10.7) of [loc. cit., page 67] is the adèlic version of the last sum where we group together the classes conjugate over $\mathrm{PA}^\times(k)$, where $\mathrm{PA}^\times$ is the group used to construct the lattice Γ as explained in Section 1D. The passage between the adèlic and classical trace formula is explained in [loc. cit., Theorem 4.21]. Proceeding as in [loc. cit., pages 67–69] we obtain the bound

$$\sum_{\substack{[\gamma]_\Gamma \\ \text{nontorsion}}} \mathrm{vol}(\Gamma_\gamma\backslash G_\gamma)\mathcal{O}_\gamma(f) \ll \mathrm{vol}(\Gamma\backslash G)^{0.986}.$$

Any hyperbolic conjugacy class $[\gamma]_\Gamma$ is nontorsion so we can deduce the that the sum (2-3) converges to 0 as $\mathrm{vol}(\Gamma\backslash X) \to \infty$ and Γ is a congruence arithmetic lattice. In order to establish the convergence for sequences of pairwise noncommensurable arithmetic lattices $(\Gamma_n)_{n\in\mathbb{N}}$ we choose for each n a maximal arithmetic lattice Λ_n containing Γ_n. It is always a congruence arithmetic lattice. We have

$$\begin{aligned}\frac{1}{\mathrm{vol}(\Gamma_n\backslash X)}\left|\sum_{[\gamma]_{\Gamma_n}\in U} \mathrm{vol}((\Gamma_n)_\gamma\backslash G_\gamma)\mathcal{O}_f(\gamma)\right| &\le \frac{1}{\mathrm{vol}(\Gamma_n\backslash X)}\sum_{[\gamma]_{\Gamma_n}\in U} \mathrm{vol}((\Gamma_n)_\gamma\backslash G_\gamma)\mathcal{O}_{|f|}(\gamma) \\ &\le \frac{1}{\mathrm{vol}(\Lambda_n\backslash X)}\sum_{[\gamma]_{\Lambda_n}\in U} \mathrm{vol}((\Lambda_n)_\gamma\backslash G_\gamma)\mathcal{O}_{|f|}(\gamma) \\ &= o(1).\end{aligned}$$

□

3. Structure of the singular locus of closed hyperbolic orbifolds

To be able to deduce from the sole Benjamini–Schramm convergence of a sequence of orbifolds further asymptotic results on topological invariants we need a fine metric description of the singular locus. The results in this section provide it; they are not really original but precise statements such as we need are not easily found in the literature. As usual our main tool is the Margulis lemma.

Theorem 3.1. *For every $n \geq 2$ there exists $\varepsilon = \varepsilon(n) > 0$ such that the following holds. Let Γ be a discrete subgroup of isometries of $\mathbb{H}^n$, then for any $x \in \mathbb{H}^n$ the subgroup*

$$\Gamma_\varepsilon := \langle \gamma \in \Gamma : d(x, \gamma x) \leq \varepsilon \rangle$$

is virtually abelian.

In the sequel we will only work in 2 or 3-dimensional hyperbolic space, and we let ε denote a Margulis constant which is valid for both cases. Recall that $O_{\leq\varepsilon}$ stands for the ε-thin part of an orbifold O, for which we use the following definition: if $O = \Gamma\backslash X$ where X is the orbifold universal cover and we assume X to be CAT(0) then

$$O_{\leq\varepsilon} = \Gamma\backslash\{\tilde{x} \in X : \exists\gamma \in \Gamma \setminus \{\mathrm{Id}\},\ d(\tilde{x}, \gamma\tilde{x}) \leq \varepsilon\} \tag{3-1}$$

which includes the singular locus of O — note that in the literature, e.g., in [Boileau et al. 2003], a different convention is often used where only points with large stabilizers are included. The closure of the complement of $O_{\leq\varepsilon}$ (the ε-thick part) will be denoted by $O_{\geq\varepsilon}$.

In fact we need to tweak a bit the definition of the thin part around that part of the singular locus where the cone angle is π: around these vertices or geodesics we put a collar whose width is $\varepsilon/6$ (instead of $\varepsilon/2$).

3A. ***2-dimensional orbifolds.*** In $\mathrm{PGL}_2(\mathbb{R})^+$ all the virtually abelian discrete subgroups are given by the following list:

(1) An infinite cyclic group generated by an hyperbolic or parabolic isometry.

(2) A finite cyclic group generated by an elliptic isometry.

(3) An infinite dihedral group generated by two elliptic isometries of order 2.

As a first consequence we see that the singular locus of an orientable hyperbolic 2-orbifold consists only of *cone points*, that is all nonmanifold points have a neighborhood which is isometric to the quotient of a disc by a finite cyclic group.

In addition we can deduce from this classification a metric description of the singular locus. We need the following notation: given an elliptic isometry γ with fixed point x and rotation angle θ, let $\ell(\theta, \varepsilon)$ be the smallest ℓ such that $d(y, \gamma y) \geq \varepsilon$ for $d(x, y) = \ell$. Similarly, given a hyperbolic isometry γ of minimal displacement ℓ we define $r(\ell, \varepsilon)$ to be the minimal distance from its axis at which an hyperbolic isometry translates of at least ε.

Lemma 3.2. *Let $O = \Gamma\backslash\mathbb{H}^2$ be an orientable hyperbolic 2-orbifold and x a point in its singular locus. Then x is an isolated cone point and one of the following possibilities hold*:

(1) *If its angle is* $2\pi/m$ *with* $m \geq 3$ *then there is no other singular point in the ball* $B_O(x, \ell)$ *where* $\ell = \ell(2\pi/m, \varepsilon)$.

(2) *If the angle is equal to* π *then either there is no other singular point within distance* $\ell(\pi, \varepsilon)$, *or there is one* (*and its cone angle is also* π) *at distance* $\ell_x < \ell(\pi, \varepsilon)$ *but no other within distance* $r(\ell_x, \varepsilon)$ *of* x.

Proof. Let $\Gamma x \in O$ be as in the statement, with $x \in \mathbb{H}^2$. Then x is a fixed point of a nontrivial element of Γ, and it follows that the subgroup

$$\Gamma_x^\varepsilon = \{\gamma \in \Gamma : d(x, \gamma x) \leq \varepsilon\}$$

must be one of those described in (2) or (3) at the beginning of this section; let γ_0 be a generator (with minimal rotation angle) of the cyclic subgroup fixing x and $m > 1$ its order.

In any case x lies above a conical point in O. Assume now that $m \geq 3$; then $\Gamma_x = \langle \gamma_0 \rangle$ and by the Margulis lemma there is no other fixed point of a nontrivial element in Γ within the set

$$C = \{y \in \mathbb{H}^2 : d(y, \gamma_0 y) \leq \varepsilon)\}.$$

By definition the ball $B_{\mathbb{H}^2}(x, \ell(2\pi/m, \varepsilon))$ is contained in C, so it contains no other singular point.

If $m = 2$ and there is another elliptic fixed point $x' \in \mathbb{H}^2$ with $d(x, x') \leq \ell(\pi, \varepsilon)$ then we might assume that x' is the closest such point. By the previous paragraph any nontrivial $\gamma_0' \in \Gamma$ fixing x' must be of order 2. Let $\eta = \gamma_0 \gamma_0'$. It is a hyperbolic isometry with axis containing the geodesic α joining x to x' and translation distance $2d(x, x')$. Write Γ_α for the setwise stabilizer of α in Γ. For every $\gamma \in \Gamma_\alpha$ not fixing x we will have $d(x, \gamma x) \geq 2d(x, x')$ as otherwise $\gamma_0 \gamma$ would have a fixed point closer to x than x'. We deduce that $\Gamma_\alpha = \langle \gamma_0, \gamma_0' \rangle$. The former is a maximal virtually abelian subgroup of Γ (it is an intersection of Γ with the normalizer of a split torus). The Margulis lemma now implies that within the ball $B_{\mathbb{H}^2}(x, \ell(\pi, \varepsilon))$ (resp. $B_{\mathbb{H}^2}(x, r(\ell_x, \varepsilon))$) any other elliptic fixed point must be a translate of either x or x' by a power of η, as any such point is moved by at most ε by γ_0 (resp. η) and hence its stabilizer in Γ must belong to Γ_α. □

3B. *3-dimensional orbifolds.*

3B1. *Description of the singular locus.* The list of discrete virtually abelian subgroups of $\mathrm{PGL}_2(\mathbb{C})$ is long enough to make us avoid giving a complete description. Rather, we will assume that Γ is a cocompact lattice in $\mathrm{PGL}_2(\mathbb{C})$ and Λ a maximal virtually abelian subgroup of Γ which contains torsion elements (which is all we need to prove Theorem C). If Λ contains a hyperbolic element γ then it must normalize $\langle \gamma \rangle$, so it is contained in the normalizer of a maximal torus. Any such normalizer is isomorphic to $\mathbb{C}^\times \rtimes \mathbb{Z}/2$. Otherwise Λ contains only elements of finite order and so by Burnside's theorem it must be a finite subgroup of the maximal compact $\mathrm{PU}(2)$. It follows that Λ is one of the following groups:

(1) $\langle \gamma, \eta \rangle \cong \mathbb{Z} \times \mathbb{Z}/m$ where γ, η are respectively hyperbolic and elliptic isometries sharing the same axis.

(2) $\langle\gamma, \eta, \rho\rangle \cong (\mathbb{Z} \times \mathbb{Z}/m) \rtimes \mathbb{Z}/2$ where η, γ are as above (with η possibly trivial) and ρ is an elliptic of order 2 with axis orthogonal to that of γ or η.

(3) One of the finitely many nondihedral finite subgroups of $\mathrm{PU}(2)$.

We see from this description that the singular locus of an hyperbolic 3-orbifold consists of closed geodesics (which we will call *singular geodesics*), which can intersect each other. A singular point not on the intersection of two singular geodesics has a neighborhood isometric to the quotient of a ball by a rotation; the angle of the latter we will call the cone angle of the singular geodesic. We will call a vertex which is at the intersection of two or more singular geodesics a *vertex* of the singular locus.

Together with the Margulis lemma the list above allows us to give the following metric description of the singular locus (see also [Boileau et al. 2003, Corollary 6.3] for a more geometric description, and [loc. cit., Figure 5 on page 33] for illustrations). This description is analogous to the situation from Lemma 3.2; we recall that ℓ and r were defined there.

Lemma 3.3. *Let O be a compact orientable 3-dimensional hyperbolic orbifold and Σ its singular locus. Let $x \in \Sigma$ be a vertex. Then one of the two following possibilities hold*:

(1) *The $\varepsilon/2$-neighborhood of x is isometric to one of a finite list of orbifolds, whose singular locus has only one vertex and all singular geodesics go through x.*

(2) *There is at most one other singular vertex x' within distance $\varepsilon/2$ of x; x and x' are joined by a singular geodesic c of length ℓ and cone angle $2\pi/m$, there are two singular geodesics with cone angle π and orthogonal to c each going through one of x or x'. There are no further components of the singular locus within distance* $\max(\ell(2\pi/m, \varepsilon), r(\ell, \varepsilon))$ *of x and x'.*

Moreover if two nonintersecting singular geodesics of O are within distance $\varepsilon/2$ of each other then both have angle π.

Proof. Let $O = \Gamma\backslash\mathbb{H}^3$ a closed hyperbolic 3-orbifold. Let x be a vertex in the singular locus of O and Π the subgroup of Γ fixing a lift $\tilde{x}$ of x to $\mathbb{H}^3$. Then Π is either a dihedral group $\mathbb{Z}/m \rtimes \mathbb{Z}/2$ or one of finitely many finite nondihedral subgroups of $\mathrm{PU}(2)$, according to the list of virtually abelian subgroups of Γ above.

If the vertex is as in (1) and $\eta \in \Gamma$, $\eta \notin \Pi$ is an elliptic isometry of order m then as (by the Margulis lemma) Π contains all isometries moving $\tilde{x}$ by at most ε any fixed point of η must be at distance at least $\ell(2\pi/m, \varepsilon) \geq \ell(\pi, \varepsilon) = \varepsilon/2$ of $\tilde{x}$. Similarly any hyperbolic isometry in Γ must move $\tilde{x}$ by at least ε. Hence the quotient $\Pi\backslash B(\tilde{x}, \varepsilon/2)$ embeds into O.

If the vertex has a dihedral stabilizer as in (2) let η be a generator of the $\mathbb{Z}/m$-subgroup and γ a generator of the $\mathbb{Z}$-subgroup commuting with η. We might assume that either $\ell < \varepsilon/2$ or $m > 5$ (otherwise we can add its neighborhood to the finite list in (1)). Then any elliptic element of Γ which does not normalize $\langle\eta\rangle$ cannot fix a point in $B(\tilde{x}, \varepsilon)$ (otherwise it and η would generate a subgroup moving a point by less than ε but not in the list given above, which is not possible by the Margulis lemma). Similarly it cannot fix a point within $r(\ell, \varepsilon)$ of the axis of γ. □

3B2. *Smoothing the thick part.* Let $C = (C_0, C_1, \dots) \in [0, +\infty[^{\mathbb{N}}$. As (a slight variation of) the definition in [Lück and Schick 1999] we say that a Riemannian manifold has *C-bounded geometry* if its injectivity radius is at least C_0, the normal geodesic flow up to C_0 gives coordinates for a collar neighborhood of the boundary, and the k-th derivatives of the metric tensor and its inverse (in normal coordinates) are bounded in sup norm by C_k. In this section we prove the following lemma.

Lemma 3.4. *There exists C such that for any hyperbolic 3-orbifold O there exists a smooth submanifold O' such that*:

- *$O_{\geq\varepsilon} \subset O'$ and this is an homotopy equivalence.*
- *O' is of C-bounded geometry.*

We will deduce the lemma from the description of the singular locus and the following general proposition, the proof of which we give in Appendix B.

Proposition 3.5. *Let X be a Riemannian d-manifold and H_1, H_2 two open subsets whose closures have smooth boundary. Assume the following hold*:

- *They intersect transversally in a compact subset*; *let α_0 such that the dihedral angles at the intersection stay within the interval $]\alpha_0, \pi - \alpha_0[$.*
- *Both manifolds $X \setminus H_i$ are of bounded geometry.*

Then for any $\delta > 0$ there exists an open subset H of X such that:

(1) *$H \supset H_1 \cup H_2$ and they are equal outside of the δ-neighborhood of $H_1 \cap H_2$.*

(2) *The closure of H has a smooth boundary.*

(3) *$X \setminus H$ is of bounded geometry*; *the bounds depend only on δ, on the bounds on the geometry of X and $X \setminus H_i$ and on α_0.*

Proof of Lemma 3.4. Observe first that the boundary of the thin part is smooth away from the geodesics with cone angle π and the vertices of the singular locus, as follows from the third part of Lemma 3.3. Thus the nonsmooth part of $\partial O_{\geq\varepsilon}$ comes from intersecting tubular neighborhoods of singular geodesics and short geodesics. There are finitely many possible configurations where the geodesics are not orthogonal to each other (corresponding to case (1) of Lemma 3.3); we do not need to deal in detail with these, so the only problem left to deal with is the following: at all points in the intersection of the tubular neighborhood N_1 (with varying radius) of one geodesic, and the $\varepsilon/6$-tubular neighborhood N_2 of another geodesic orthogonal to the first, the dihedral angle between ∂N_1 and ∂N_2 stays bounded away from 0 and from π.[1]

To prove this note that the maximum and minimum values for these angles both are continuous functions of the radius $0 \leq r < +\infty$ of N_1. It can be continuously extended to $r = +\infty$, the values then being those of the angle (in a conformal model of $\mathbb{H}^3$) between ∂N_1 and the boundary at infinity of $\mathbb{H}^3$. As N_1

[1]Note that the neighborhoods corresponding to two geodesics orthogonal to a third one cannot intersect each other, because we took their radius to be $\varepsilon/3$ and the distance between the geodesics outside the ε-thin part is at least $\varepsilon/2$

and N_2 are never tangent to each other we see by compactness that the maximal and minimal values stay bounded away from 0 and π. □

4. The genus of congruence orbifolds

In this section we prove Theorem B. Let O be an hyperbolic orbifold of dimension 2, which is a quotient of the hyperbolic plane $\mathbb{H}^2$ by a lattice of $\mathrm{PSL}_2(\mathbb{R})$. Then the underlying topological space $|O|$ is a surface of finite type, that is it is homeomorphic to a compact surface S with a finite number of points removed. The *genus* of O is defined to be the genus of S.

Suppose that O has genus g, k punctures and r conical singularities with angles $2\pi/m_1, \dots, 2\pi/m_r$ (the tuple $(g, k, m_1, \dots, m_r)$ is then called the *signature* of O). Then, computing the volume of a well-chosen fundamental polygon we get the following equality (see [Beardon 1983, Theorem 10.4.2]):

$$\operatorname{vol} O = 2\pi\left(2g - 2 + k + \sum_{i=1}^{r}\left(1 - \frac{1}{m_i}\right)\right). \tag{4-1}$$

From this equation we obtain the bound:

$$\left| g - \frac{\operatorname{vol}(O)}{4\pi} \right| \le \frac{k + r + 2}{4\pi}.$$

We now see that Theorem B follows from Theorem A together with the following proposition.

Proposition 4.1. *Let O_n be a sequence of hyperbolic 2–orbifolds which is Benjamini–Schramm convergent to $\mathbb{H}^2$. Let k_n, r_n be the numbers of cusps and conical points of O_n, respectively. Then $k_n + r_n = o(\operatorname{vol} O_n)$.*

Proof. To prove that $r_n = o(\operatorname{vol} O_n)$ we associate to each conical point x with angle θ the region

$$\Omega_x = B(x, \ell(\theta, \varepsilon))$$

if there is no other singular point within distance $\ell(\theta, \varepsilon)$. Otherwise let ℓ_x be the distance to the nearest singular point and put

$$\Omega_x = B(x, r(\ell_x, \varepsilon)).$$

We will check below the following facts:

(1) There exists $c > 0$ such that $\operatorname{vol} \Omega_x > c$ for all n and $x \in O_n$.

(2) Any point $p \in O_n$ is covered by at most two distinct sets Ω_x.

(3) For all conical points $x \in O_n$ we have $\Omega_x \subset (O_n)_{\le\varepsilon}$.

It follows from these that

$$r_n \le \frac{1}{c} \sum_{x \in \Sigma_{O_n}} \operatorname{vol} \Omega_x \le \frac{2}{c} \operatorname{vol}\left(\bigcup_{x \in \Sigma_{O_n}} \Omega_x \right) \le \frac{2}{c} \operatorname{vol}(O_n)_{\le\varepsilon}$$

and as the right-hand side is $o(\operatorname{vol} O_n)$ in a BS-convergent sequence we get that $r_n = o(\operatorname{vol} O_n)$.

That (3) holds follows immediately from the definitions of $\ell(\theta,\varepsilon)$ and $r(\ell,\varepsilon)$. Point (2) follows from the Margulis lemma combined with Lemma 3.2.

It remains to prove (1). Let $x \in O_n$ be a singularity with cone angle $2\pi/m$ with $m > 2$, let $\tilde{x}$ be a lift of x to $\mathbb{H}^2$ and $\ell = \ell(2\pi/m, \varepsilon)$. Then we have

$$\mathrm{vol}(B_{O_n}(x,\ell)) = \frac{1}{m} B_{\mathbb{H}^2}(\tilde{x},\ell) \gg \frac{e^\ell}{m}$$

so we need to prove that $e^\ell \gg m$. This follows easily from distance computations in the disk model: by definition of $\ell(\theta,\varepsilon)$ we have that $\ell(\theta,\varepsilon) = \log((1+r)/(1-r))$ where $0 < r < 1$ is such that $d(r, re^{i\theta}) = \varepsilon$. It follows that

$$\cosh(\varepsilon) = 1 + \frac{2r^2|1-e^{i\theta}|^2}{(1-r^2)^2}$$

and by standard computations we get that

$$r = 1 - \frac{\theta}{\sqrt{2}\sinh(\varepsilon)} + O(\theta^2)$$

whence it follows that

$$\ell(\theta,\varepsilon) = -\log(\theta) - c + O(\theta)$$

for some constant c depending on ε. We finally get that $\ell \gg e^{\log(m/2\pi)} \gg m$.

Assume now that $m = 2$ and that there is another singular point x' within $\ell(2,\varepsilon)$ of x. In this case the volume of Ω_x is half that of a collar around a closed geodesic of length $r(\ell_x,\varepsilon) \ll \varepsilon$; as the latter is bounded from below (see [Halpern 1981]) so is that of Ω_x.

The proof that $k_n = o(\mathrm{vol}\, O_n)$ is similar: by the Margulis lemma the regions of the ε-thin part where a given conjugacy class of parabolic isometries realizes the injectivity radius are pairwise disjoint, and an easy hyperbolic area computation shows that the volume of such a region is bounded below. □

5. Betti numbers of arithmetic 3-orbifolds

Recall that ε is the Margulis constant for $\mathbb{H}^3$. Let O be a 3-orbifold, then we will write O' for the manifold with boundary obtained by Lemma 3.4. We write Δ^1_{abs} for the maximal self-adjoint extension of the Hodge–Laplace operator on O' with absolute boundary condition. The goal of this section is to prove the following proposition, which we do by extending the analysis at the end of section 7 in [Abert et al. 2017] to the orbifold case.

Proposition 5.1. *Let O_n be a sequence of closed hyperbolic 3-orbifolds which BS-converge to $\mathbb{H}^3$, and let O'_n be the smoothings described in Lemma 3.4. Then for all $t > 0$ we have that*

$$\limsup_{t\to+\infty} \lim_{n\to+\infty} \frac{\mathrm{Tr}(e^{-t\Delta^1_{\mathrm{abs}}[O'_n]})}{\mathrm{vol}\, O_n} = 0.$$

Before giving the proof we explain how this implies Theorem C: let $O_n = \Gamma_n\backslash\mathbb{H}^3$. By Hodge theory we have $b_1(O'_n) \le \mathrm{Tr}(e^{-t\Delta^1_{\mathrm{abs}}[O'_n]})$ for all t, and so Proposition 5.1 implies that

$$\lim_{n\to+\infty} \frac{b_1(O'_n)}{\mathrm{vol}\, O_n} = 0.$$

On the other hand we have that the orbifold fundamental group Γ_n is a quotient of $\pi_1(O'_n)$. Indeed, the universal cover of $(O_n)_{\ge\varepsilon}$ is a cover of the connected subset $(\hat{O}_n)_{\ge\varepsilon}$ of those $x \in \mathbb{H}^3$ which are not displaced by less than ε by some nontrivial element of Γ_n, and $(O_n)_{\ge\varepsilon}$ is homotopy equivalent to O'_n. Moreover $H_1(O'_n)$ is the abelianization of $\pi_1(O'_n)$. From these two facts it follows that $b_1(\Gamma_n) \le b_1(O'_n)$, so that $b_1(\Gamma_n) = o(\mathrm{vol}\, O_n)$ as well.

The proof of Proposition 5.1 is done in four steps: first we prove an analogue of Proposition 4.1 and then deduce the convergence of the part of the trace formula for O_n coming from the ε-thick part: see (5-1). The two next steps together imply that the trace of the heat kernel on O'_n is asymptotically the same as that computed in (5-1): first we analyze the integral of the difference on the R-thick part and show that it limit superior is $o(R)$ (see (5-6), then we prove that the integral on the R-thin part of O'_n asymptotically vanishes (see (5-7)). Altogether these three steps imply that

$$\lim_{n\to+\infty} \frac{\mathrm{Tr}(e^{-t\Delta^1_{\mathrm{abs}}[O'_n]})}{\mathrm{vol}\, O_n} = \mathrm{tr}\, e^{-t\Delta^1[\mathbb{H}^3]}$$

where we denoted $\mathrm{tr}\, e^{-t\Delta^1[\mathbb{H}^3]} = \mathrm{tr}\, e^{-t\Delta^1[\mathbb{H}^3]}(\tilde{x},\tilde{x})$ for any $\tilde{x} \in \mathbb{H}^3$. The proposition now follows from the vanishing of the first L^2-Betti number of $\mathbb{H}^3$, which means that $\lim_{t\to+\infty} \mathrm{tr}\, e^{-t\Delta^1[\mathbb{H}^3]} = 0$ (see [Lück 2002]).

5A. ***Upper bound on the total length of singular geodesics.*** Let Σ_n be the set of singular geodesics of O_n. To prove Proposition 5.1 we will need to control the total length $\sum_{c\in\Sigma_n} \ell_n$ in terms of the volume of the thin part of O_n. This is problematic for 3-orbifolds because of an issue with singular geodesics corresponding to order-2 elements. For these geodesics we will need to replace the lengths in the sum by another quantity. To make it precise let us introduce some notations.

Let O by a finite volume hyperbolic 3-orbifold and let Σ be the set of singular geodesics on O. For $c \in \Sigma$ we will write $\tilde{c}$ for a lift of c to $\mathbb{H}^3$; in our arguments below we will clarify the choice of $\tilde{c}$ whenever it matters. Let Γ be the orbifold fundamental group of O. Let $c \in \Sigma$ and write $\Gamma_{\tilde{c}}$ for the pointwise stabilizer of its lift $\tilde{c}$. Then $\Gamma_{\tilde{c}}$ is a lattice inside a maximal torus of $\mathrm{PGL}(2,\mathbb{C})$, so is it is of the form $\mathbb{Z}\times\mathbb{Z}/m_c$ for an integer $m_c \ge 2$. We write ℓ_c for the length of c.

Let M be the maximal order of a finite nondihedral subgroup of $\mathrm{PU}(2)$. The relevance of M to the arguments below comes from the fact that finite subgroups of $\mathrm{PGL}(2,\mathbb{C})$ either stabilize a geodesic in $\mathbb{H}^3$ or are conjugate to a nondihedral subgroup of $\mathrm{PU}(2)$. Accordingly, we divide Σ into three sets Σ^1, Σ^2, Σ^3 defined as follows:

$$\Sigma^1 = \{c \in \Sigma \mid m_c = 2\}, \quad \Sigma^2 = \{c \in \Sigma \mid 2 < m_c \le M\}, \quad \Sigma^3 = \{c \in \Sigma \mid M < m_c\}.$$

The sets do not depend on the choice of $\tilde{c}$. Let $c \in \Sigma^1$. A point $p \in c$ will be called a *type* I *vertex* if there exists a closed geodesic $a \notin \Sigma^3$ on O (not necessarily singular) such that $p \in c \cap a$ and $\ell_a \leq \varepsilon$. A point $p \in c$ is a *type* II *vertex* if there exists $b \in \Sigma^3$ such that $p \in c \cap b$. Write $T^{\mathrm{I}}(c)$, $T^{\mathrm{II}}(c)$ for the sets of type I and type II vertices. For $p \in T^{\mathrm{I}}(c)$, $T^{\mathrm{II}}(c)$ we let $r_p := \max\{r(\ell_a, \varepsilon), \ell(2\pi/m_a, \varepsilon)\}, \max\{r(\ell_b, \varepsilon), \ell(2\pi/m_b, \varepsilon)\}$ respectively. Define $\ell'_c := \ell_c - \sum_{p \in T^{\mathrm{II}}(c)} 2r_p$.

Proposition 5.2. *For any hyperbolic* 3*-orbifold O we have*

$$\sum_{c \in \Sigma \setminus \Sigma^1} \ell_c + \sum_{c \in \Sigma^1} (\ell'_c + |T^{\mathrm{II}}(c)|) \ll \mathrm{vol}(O_{\leq \varepsilon}).$$

Proof. As in the proof of Proposition 4.1 we will construct sets $\Omega_c, \Omega_p^{\mathrm{II}} \subset O$ attached to each singular geodesic $c \in \Sigma$ and to $p \in T^{\mathrm{II}}(c)$ for $c \in \Sigma^1$ satisfying the following properties:

(1) For $c \in \Sigma \setminus \Sigma^1$ we have $\mathrm{vol}(\Omega_c) \gg \ell_c$; for $c \in \Sigma^1$ we have $\mathrm{vol}(\Omega_c) \gg \ell'_c$ and for $p \in T^{\mathrm{II}}(c)$ $\mathrm{vol}(\Omega_p^{\mathrm{II}}) \gg 1$.

(2) Any point $x \in O$ is covered by at most M distinct sets $\Omega_c, \Omega_p^{\mathrm{II}}$.

(3) $\Omega_c, \Omega_p^{\mathrm{II}} \subset O_{\leq \varepsilon}$.

If $A \subset \mathbb{H}^3$ write $[A]$ for the image of A in O under the covering map. The subset Σ^1 is the most problematic so let us first define the sets Ω_c for $c \in \Sigma^2, \Sigma^3$:

- For $c \in \Sigma^3$ let $\Omega_c := [B_{\mathbb{H}^3}(\tilde{c}, \ell(2\pi/m_c, \varepsilon))]$.
- For $c \in \Sigma^2$ let $\Omega_c := [B_{\mathbb{H}^3}(\tilde{c}, \varepsilon/2)]$.

Now let $c \in \Sigma^1$. We construct sets $\Omega_p^{\mathrm{I}}, \Omega_p^{\mathrm{II}}$ for $p \in T^{\mathrm{I}}(c), T^{\mathrm{II}}(c)$ respectively:

- $\Omega_p^{\mathrm{I}} = [B_{\mathbb{H}^3}(\tilde{a}, r(\ell_a, \varepsilon))]$.
- $\Omega_p^{\mathrm{II}} = [B_{\mathbb{H}^3}(\tilde{b}, r_p)]$ (recall that $\max\{r(\ell_b, \varepsilon), \ell(2\pi/m_b, \varepsilon)\}$).

The Margulis lemma and the description of nilpotent subgroups from Section 3B1 imply that $\Omega_p^{\mathrm{I}}, \Omega_q^{\mathrm{II}}$ are pairwise disjoint if $p \in T^I(c)$, $q \in T^{\mathrm{II}}(c)$. We define

$$\Omega_c := [B_{\mathbb{H}^3}(\tilde{c}, \varepsilon/2)] \cup \bigcup_{p \in T^{\mathrm{I}}(c)} \Omega_p^{\mathrm{I}} \setminus \bigcup_{p \in T^{\mathrm{II}}(c)} \Omega_p^{\mathrm{II}}.$$

5A1. *Step 1.* We verify condition (1). Recall that in the proof of Proposition 4.1 we showed that $e^{\ell(2\pi/m,\varepsilon)} \gg m$. For $c \in \Sigma^3$ the formula for integration in cylindrical coordinates [Fenchel 1989, page 205] yields

$$\mathrm{vol}(\Gamma_{\tilde{c}} \backslash B_{\mathbb{H}^3}(\tilde{c}, \ell(2\pi/m_c, \varepsilon)) \gg e^{2\ell(2\pi/m_c,\varepsilon)} \ell_c m_c^{-1} \gg \ell_c.$$

Using the Margulis lemma and the description of nilpotent subgroups from Section 3B1 we can show that the map

$$\Gamma_{\tilde{c}} \backslash B_{\mathbb{H}^3}(\tilde{c}, \ell(2\pi/m_c, \varepsilon)) \to [\Gamma_{\tilde{c}} \backslash B_{\mathbb{H}^3}(\tilde{c}, \ell(2\pi/m_c, \varepsilon))] = \Omega_c$$

is at most 2-to-1, so $\mathrm{vol}(\Omega_c) \gg \ell_c$.

For $c \in \Sigma^2$ we similarly get

$$\mathrm{vol}(\Gamma_{\tilde{c}} \backslash B_{\mathbb{H}^3}(\tilde{c}, \ell(2\pi/m_c, \varepsilon)) \gg \ell_c.$$

By Lemma 3.3 and the Margulis lemma the map

$$\Gamma_{\tilde{c}} \backslash B_{\mathbb{H}^3}(\tilde{c}, \varepsilon/2) \to [\Gamma_{\tilde{c}} \backslash B_{\mathbb{H}^3}(\tilde{c}, \varepsilon/2)]$$

is at most M-to-one. Hence $\mathrm{vol}(\Omega_c) \gg \ell_c$.

Now let $c \in \Sigma^1$. Since the sets $\Omega^{\mathrm{I}}_p, \Omega^{\mathrm{II}}_q$ for $p \in T^I(c)$, $q \in T^{\mathrm{II}}(c)$ are pairwise disjoint we can write

$$\ell_c = \ell'_c + \sum_{p \in T^{\mathrm{II}}(c)} 2r_p \quad \text{and} \quad \ell'_c = \ell''_c + \sum_{p \in T^I(c)} 2r_p$$

where $\ell''_c \geq 0$. Let $p \in T^I(c)$. Let γ be an element of $\Gamma_{\tilde{a}}$ translating $\tilde{a}$ by ℓ_a. Integration in cylindrical coordinates yields

$$\mathrm{vol}(\langle\gamma\rangle \backslash B_{\mathbb{H}^3}(\tilde{a}, r_p) \gg \ell_a^{-1} \gg r_p.$$

Note that we implicitly used here the fact that m_a is bounded. The Margulis lemma implies that the quotient map from the last set to $[B_{\mathbb{H}^3}(\tilde{a}, r(\ell_a, \varepsilon))]$ is at most M-to-1 so we deduce $\mathrm{vol}(\Omega^{\mathrm{I}}_p) \gg r_p$. Reasoning as in the previous cases we get $\mathrm{vol}(\Omega_c) \gg \ell''_c + \sum_{p \in T^I(c)} r_p \gg \ell'_c$.

Finally let $p \in T^{\mathrm{II}}(c)$. Integrating in cylindrical coordinates we get

$$\mathrm{vol}(\Gamma_b \backslash B_{\mathbb{H}^3}(\tilde{b}, \max\{r(\ell_b, \varepsilon), \ell(2\pi/m_b, \varepsilon)) \gg \frac{\ell_b}{m_b} \max\{m_b^2, \ell_b^{-2}\} \gg 1.$$

As before we deduce $\mathrm{vol}(\Omega^{\mathrm{II}}_p) \gg 1$. This concludes the first step.

5A2. *Step 2.* We verify condition (2). For $c \in \Sigma^3$ the sets Ω_c are pairwise disjoint. Indeed let $c_1, c_2 \in \Sigma^3$ and assume $\Omega_{c_1} \cap \Omega_{c_2} \neq \varnothing$. By the Margulis lemma, for some lifts $\tilde{c}_1, \tilde{c}_2$ the torsion parts of the stabilizers $\Gamma_{\tilde{c}_1}, \Gamma_{\tilde{c}_2}$ generate a nilpotent subgroup. By discussion in Section 3B1 it is either contained in a normalizer of geodesic or in a finite nondihedral subgroup of $\mathrm{PU}(2)$, and the definition of Σ^3 excludes the second option so $\Gamma_{\tilde{c}_1}, \Gamma_{\tilde{c}_2}$ both normalize the same geodesic. This can happen only if $\tilde{c}_1 = \tilde{c}_2$.

A similar argument shows that for $c_1 \in \Sigma^2$, $c_2 \in \Sigma^3$ the sets $\Omega_{c_1}, \Omega_{c_2}$ are disjoint.

By Lemma 3.3 and the Margulis lemma the sets Ω^{II}_p are pairwise disjoint or equal. It is not hard to verify that we can have at most two different $p \in T^{\mathrm{II}}(c)$, $p' \in T^{\mathrm{II}}(c')$ such that $\Omega^{\mathrm{II}}_p = \Omega^{\mathrm{II}}_{p'}$. By construction Ω^{II}_p contains exactly one set of form Ω_c with $c \in \Sigma^3$. By Lemma 3.3 together with the Margulis lemma Ω^{II}_p are disjoint from Ω_c if $c \in \Sigma^1, \Sigma^2$. Again by the Margulis lemma and Lemma 3.3, every point $x \in O$ can be covered by at most M sets Ω_c with $c \in \Sigma^1, \Sigma^2$. We conclude that any point is covered by at most M distinct sets of form Ω_c, $c \in \Sigma$ and Ω^{II}_p, $p \in T^{\mathrm{II}}(c)$, $c \in \Sigma^3$.

5A3. *Last step.* Property (3) holds by construction. We get

$$\sum_{c \in \Sigma} \mathrm{vol}(\Omega_c) + \sum_{c \in \Sigma^3} \sum_{p \in T^{\mathrm{II}}(c)} \mathrm{vol}(\Omega^{\mathrm{II}}_p) \ll M \, \mathrm{vol}(O_{\leq\varepsilon}).$$

By the first step we conclude that

$$\sum_{c\in\Sigma\setminus\Sigma^1}\ell_c+\sum_{c\in\Sigma^1}\big(\ell_c'+|T^{\mathrm{II}}(c)|\big)\ll \mathrm{vol}(O_{\le\varepsilon}).\qquad\square$$

5B. ***Trace formula on the thick part.*** Let O_n be a sequence as in Proposition 5.1. We prove here that

$$\int_{(O_n)_{\ge\varepsilon}}\operatorname{tr}e^{-t\Delta^1[O_n]}(x,x)\,dx-\operatorname{tr}e^{-t\Delta^1[\mathbb{H}^3]}\cdot\mathrm{vol}\,O_n=o(\mathrm{vol}\,O_n).\tag{5-1}$$

Let $\mathcal{C}_{n,e}$ and $\mathcal{C}_{n,h}$ be the sets of conjugacy classes of respectively elliptic and hyperbolic elements in Γ_n. For $\gamma\in\Gamma$ let $\mathcal{F}_\gamma$ be a fundamental domain for the centralizer Γ_γ of γ in Γ and $\mathcal{F}_\gamma^{\ge\varepsilon}$ the part of it on which the nontrivial elements of Γ displace by at least ε. The proof of the Selberg trace formula then gives that

$$\int_{(O_n)_{\ge\varepsilon}}\operatorname{tr}e^{-t\Delta^1[O_n]}(x,x)\,dx=\mathrm{vol}(O_n)_{\ge\varepsilon}\operatorname{tr}e^{-t\Delta^1[\mathbb{H}^3]}+\sum_{[\gamma]\in\mathcal{C}_{n,e}\cup\mathcal{C}_{n,h}}\int_{\mathcal{F}_\gamma^{\ge\varepsilon}}\operatorname{tr}(\gamma^*e^{-t\Delta^1[\mathbb{H}^3]}(x,\gamma x))\,dx.\tag{5-2}$$

Because of Benjamini–Schramm convergence we have $\mathrm{vol}\,O_n-\mathrm{vol}(O_n)_{\ge\varepsilon}=o(\mathrm{vol}\,O_n)$. Then (5-1) will follow from (5-2) together with the following limit:

$$\sum_{[\gamma]\in\mathcal{C}_{n,e}\cup\mathcal{C}_{n,h}}\int_{\mathcal{F}_\gamma^{\ge\varepsilon}}\operatorname{tr}(\gamma^*e^{-t\Delta^1[\mathbb{H}^3]}(x,\gamma x))\,dx=o(\mathrm{vol}\,O_n).\tag{5-3}$$

We proceed to prove (5-3). The proof for the hyperbolic part is exactly the same as in [Abert et al. 2017, Section 7].

We deal now with the elliptic part; similar computations are done in [Elstrodt et al. 1998, pages 193 and following]. To simplify the computations we integrate over a subset $\mathcal{E}_\gamma^{\ge\varepsilon}$ of $\mathcal{F}_\gamma$ which is slightly larger than $\mathcal{F}_\gamma^{\ge\varepsilon}$.

If $[\gamma]$ is an elliptic conjugacy class let c be the singular geodesic on O_n corresponding to γ and $\tilde{c}$ the lift of c to $\mathbb{H}^3$ which is fixed by γ. Let ℓ_c be the length of c and m_c the order of the torsion subgroup of Γ_γ. If $m_c>2$ we put

$$\mathcal{E}_\gamma^{\ge\varepsilon}=\mathcal{F}_\gamma\setminus B_{\mathbb{H}^3}(\tilde{c},\max\{r(\ell_c,\varepsilon),\ell(2\pi/m_c,\varepsilon)\}).$$

The definition for γ with $m_c=2$ is bit more involved. Recall from Proposition 5.2 that we call a point $p\in c$ a type II vertex if there exists a singular geodesic b in O_n such that $p\in c\cap b$ and the torsion part of $\Gamma_{\tilde{b}}$ is of order at least M (a constant defined there). Write $T^{\mathrm{II}}(c)$ for the set of type II vertices on c. For each point $p\in T^{\mathrm{II}}(c)$ the geodesic b is unique so the values ℓ_b,m_b are well defined. To shorten notation we will write $r_c:=\max\{r(\ell_c,\varepsilon),\ell(2\pi/m_c)\}$ and $r_p:=\max\{r(\ell_b,\varepsilon),\ell(2\pi/m_b)\}$. Let $T^{\mathrm{II}}(\tilde{c})\subset\tilde{c}$ be the set of lifts of $p\in T^{\mathrm{II}}(c)$. Set $T^{\mathrm{II}}(\tilde{c})$ is Γ_γ invariant. Define

$$\mathcal{E}_\gamma^{\ge\varepsilon}:=\mathcal{F}_\gamma\setminus\Bigg(B_{\mathbb{H}^3}(\tilde{c},r_c)\cup\bigcup_{\tilde{p}\in T^{\mathrm{II}}(\tilde{c})}B_{\mathbb{H}}(\tilde{p},r_p)\Bigg).$$

We are ready to bound the integrals in (5-3) corresponding to the elliptic elements. For γ with $m_c > 2$ we have

$$e \cdot \int_{\mathcal{E}_\gamma^{\geq\varepsilon}} \operatorname{tr}(\gamma^* e^{-t\Delta^1[\mathbb{H}^3]}(x,\gamma x))\,dx = \frac{2\pi}{m_c}\ell_c \int_{\max(\ell(2\pi/m_c,\varepsilon),r(\ell_\gamma,\varepsilon))}^{+\infty} f_\theta(r)\,dr$$

where $f_\theta(r) = \sinh(r)\cosh(r)\operatorname{tr}(\gamma^* e^{-t\Delta[\mathbb{H}^3]}(x,\gamma x))$ for a point x at distance r from the axis, and $e = 1$ or $\frac{1}{2}$ according to whether $\Gamma_\gamma \cong \mathbb{Z}\times\mathbb{Z}/m$ or $(\mathbb{Z}\times\mathbb{Z}/m)\rtimes\mathbb{Z}/2$ (see 3B1 for the geometric significance of this). This is a consequence of disintegration of hyperbolic volume in cylindrical coordinates [Fenchel 1989, page 205]. By the Gaussian estimate of the heat kernel of $\mathbb{H}^3$ (which can be seen from its explicit expression; see [Taylor 2011, Proposition 2.2 on page 425] for a more general statement) we have that

$$f_{2\pi/m_c}(r) \ll C(t)e^{-c(t)r^2}$$

uniformly for $r \geq \ell(2\pi/m_c,\varepsilon)$. We get

$$\int_{\mathcal{E}_\gamma^{\geq\varepsilon}} \operatorname{tr}(\gamma^* e^{-t\Delta^1[\mathbb{H}^3]}(x,\gamma x))\,dx \ll \frac{\ell_c}{m_c}. \tag{5-4}$$

Now let γ be an elliptic element of order 2. The singular geodesic c can be identified with its lift to $\mathcal{F}_\gamma$. Let $\mathrm{pr}\colon \mathcal{F}_\gamma \to c$ be the "closest point projection" to c. By triangle inequality, for every point $y \in \mathcal{E}_\gamma^{\geq\varepsilon}$ we have $d(y,\mathrm{pr}(y)) \geq \max\{r_c, r_p - d(\mathrm{pr}(y),p) \mid p \in T^{\mathrm{II}}(c)\}$. Let ℓ'_c be as in Proposition 5.2 and let $r_p := \max\{\ell(2\pi/m_b,\varepsilon), r(\ell_b,\varepsilon)\}$ where b is the singular geodesic of O such that $p \in c\cap b$ (see the definition of type II vertices). Write $c_0 = c \setminus \bigcup_{p\in T^{\mathrm{II}}(c)} B(p,r_p)$ and $c_1 := c\setminus c_0$. Note that ℓ'_c is the length of c_0. We will split the integral over $\mathcal{E}_\gamma^{\geq\varepsilon}$ according to whether $\mathrm{pr}(y)$ falls into c_0 or c_1:

$$\begin{aligned} e\cdot\int_{\mathcal{E}_\gamma^{\geq\varepsilon}} \operatorname{tr}(\gamma^* e^{-t\Delta^1[\mathbb{H}^3]}(x,\gamma x))\,dx &= \int_{\mathrm{pr}^{-1}(c_0)\cap\mathcal{E}_\gamma^{\geq\varepsilon}} f_\pi(d(y,\mathrm{pr}(y)))\,dy + \int_{\mathrm{pr}^{-1}(c_1)\cap\mathcal{E}_\gamma^{\geq\varepsilon}} f_\pi(d(y,\mathrm{pr}(y)))\,dy \\ &\leq \pi\ell'_c \int_{\max(\ell(2\pi/m_c,\varepsilon),r(\ell_c,\varepsilon))}^{+\infty} f_\pi(r)\,dr + \pi\sum_{p\in T^{\mathrm{II}}(c)} 2\int_0^{r_p}\int_s^{+\infty} f_\pi(r)\,dr\,ds. \end{aligned}$$

Using the estimate for the heat kernel we get

$$\int_{\mathcal{E}_\gamma^{\geq\varepsilon}} \operatorname{tr}(\gamma^* e^{-t\Delta^1[\mathbb{H}^3]}(x,\gamma x))\,dx \ll \ell'_c + |T^{\mathrm{II}}(c)|. \tag{5-5}$$

Let Σ_n be the set of singular geodesics in O_n (so each is the image of an axis of an elliptic conjugacy class in Γ_n) with subsets Σ_n^1, Σ_n^2, Σ_n^3 defined as in Section 5A. If γ is an elliptic isometry of order m, primitive in Γ, there are $m-1$ elliptic elements in Γ_γ sharing the same axis. We have $\mathcal{F}_\gamma^{\geq\varepsilon} \subset \mathcal{E}_\gamma^{\geq\varepsilon}$ so by (5-4) and (5-5) we get that

$$\sum_{[\gamma]\in\mathcal{C}_{n,e}} \int_{\mathcal{F}_\gamma^{\geq\varepsilon}} \operatorname{tr}(\gamma^* e^{-t\Delta^1[\mathbb{H}^3]}(x,\gamma x))\,dx \ll \sum_{c\in\Sigma_n^2,\Sigma_n^3} \ell_c\frac{m_c-1}{m_c} + \sum_{c\in\Sigma_n^1}(\ell'_c + |T^{\mathrm{II}}(c)|).$$

It follows that

$$\sum_{[\gamma]\in\mathcal{C}_{n,e}} \int_{\mathcal{F}_\gamma^{\geq\varepsilon}} \operatorname{tr}(\gamma^* e^{-t\Delta^1[\mathbb{H}^3]}(x,\gamma x))\,dx \ll \sum_{c\in\Sigma_n\setminus\Sigma_n^1} \ell_c + \sum_{c\in\Sigma_n^1} (\ell'_c + |T^{\mathrm{II}}(c)|).$$

By Proposition 5.2 the right hand side is of order $O(\operatorname{vol}((O_n)_{\leq\varepsilon}))$. The sequence converges Benjamini–Schramm to $\mathbb{H}^3$ so $\operatorname{vol}((O_n)_{\leq\varepsilon}) = o(\operatorname{vol}(O_n))$. Estimate (5-3) follows.

5C. ***Comparison between heat kernels.*** We prove here that

$$\lim_{R\to+\infty} \limsup_{n\to+\infty} \frac{1}{\operatorname{vol} O_n} \int_{(O_n)_{\geq R}} \operatorname{tr}(e^{-t\Delta^1[O_n]} - e^{-t\Delta^1_{\mathrm{abs}}[O'_n]})(x,x)\,dx = 0. \tag{5-6}$$

To do this we let U_n be the subset of $\mathbb{H}^3$ covering O'_n and choose a fundamental domain D_n for Γ acting in the subset of U_n covering $(O_n)_{\geq R}$ (we assume R is large enough so that $(O_n)_{\geq R} \subset O'_n$). Then we can write

$$\begin{aligned}\int_{(O_n)_{\geq R}} \operatorname{tr}(e^{-t\Delta^1[O_n]} - e^{-t\Delta^1_{\mathrm{abs}}[O'_n]})(x,x)\,dx &= \int_{D_n} \sum_{\gamma\in\Gamma} \operatorname{tr}\gamma^*(e^{-t\Delta^1[\mathbb{H}^3]} - e^{-t\Delta_{\mathrm{abs}}[U_n]})(x,\gamma x)\,dx \\ &\ll e^{-\frac{R^2}{Ct}} \int_{D_n} \sum_{\gamma\in\Gamma} e^{-d(x,\gamma x)^2/(Ct)}\,dx\end{aligned}$$

where $\Delta_{\mathrm{abs}}[U_n]$ is the Laplacian with absolute boundary conditions on the complete manifold U_n, and the second line follows from [Lück and Schick 1999, Theorem 2.26]. By the same arguments as used above to demonstrate (5-1) the integral is $O(\operatorname{vol} O_n)$ (with a constant independent of R as the domain of integration shrinks when we take R to infinity). In the end we get that

$$\limsup_{n\to+\infty} \frac{1}{\operatorname{vol} O_n} \int_{(O_n)_{\geq R}} \operatorname{tr}(e^{-t\Delta^1_{\mathrm{abs}}[O_n]} - e^{-t\Delta^1[O'_n]})(x,x)\,dx \ll e^{-R^2/(Ct)}$$

from which (5-6) follows immediately.

5D. ***Heat kernel near the boundary.*** Here we prove the final ingredient for the proof of Proposition 5.1: for all $R > 0$ we have

$$\int_{O'_n\setminus(O_n)_{\geq R}} \operatorname{tr} e^{-t\Delta^1_{\mathrm{abs}}[O'_n]}(x,x)\,dx = o(\operatorname{vol} O_n). \tag{5-7}$$

By Benjamini–Schramm convergence we have that $\operatorname{vol}(O'_n \setminus (O_n)_{\geq R}) = o(\operatorname{vol} O_n)$. So to prove (5-6) it suffices to see that $\operatorname{tr} e^{-t\Delta^1_{\mathrm{abs}}[O'_n]}(x,x) = O_t(1)$ for $x \in O'_n$. As in [Abert et al. 2017, (7.19.4)] this follows from [Lück and Schick 1999, Theorem 2.35]; the latter is applicable with a uniform constant in our context by Lemma 3.4.

Appendix A: Benjamini–Schramm convergence in Gromov-hyperbolic spaces

AA. ***Orbital integrals on hyperbolic spaces.*** Let X be a proper Gromov-hyperbolic space and $G = \operatorname{Isom}(X)$. With the compact-open topology G is a locally compact second countable topological group.

For $\gamma \in G$ we denote by G_γ its centralizer. The following lemma is a slight generalization of [Bridson and Haefliger 1999, Corollary 3.10(2) on page 463] — the latter dealing only with discrete groups. It might be possible to straightforwardly adapt the arguments in [loc. cit.] to our case, but we give a different, mostly self-contained proof.

Lemma A.1. *Let $\gamma \in G$ be an hyperbolic isometry. Then $G_\gamma/\langle\gamma\rangle$ is compact.*

For the proof we use the following lemma, which should be standard but we could not find in the literature. The proof is a bit long and technical so we put it at the end of this appendix (see Section AC).

Lemma A.2. *Let γ be an hyperbolic isometry of X. For any $x \in X$ there exists constants $C = C(x, \gamma, \delta)$ and $A = A(x, \gamma, \delta)$ such that for any $y \in X$ and any k sufficiently large (depending on γ, x, δ) we have*

$$d(y, \gamma^k y) \geq Ck + 2d(y, \langle\gamma\rangle x) - A.$$

Proof of Lemma A.1. Let $\tau = d(\gamma) := \inf\{d(y, \gamma y) \mid y \in X\}$ be the minimal displacement of γ. Fix $x \in X$, let k, A, C as given by Lemma A.2 and define:

$$D = \{y \in X \mid d(y, \gamma^k y) \leq k\tau + 1\}.$$

It is a nonempty (by definition of τ) closed G_γ-invariant subset of X. Given that the action of G_γ on D is proper, the lemma will follow once we prove that $\langle\gamma\rangle\backslash D$ is compact. The previous lemma implies that

$$D \subset \{y \in X : d(y, \langle\gamma\rangle x) \leq (\tau - C)k + A + 1\}$$

so that $D \subset \gamma^{\mathbb{Z}} B(x, R)$ for some sufficiently large R, and as X is proper this in turn implies that $\langle\gamma\rangle\backslash D$ is compact. □

Let dg be a fixed Haar measure on G. According to the lemma above the subgroup G_γ admits a lattice so it is unimodular and we have a decomposition $dg = dx dh$ where dx is a G-invariant measure on G/G_γ and dh a Haar measure on G_γ, both depending only on the original choice of dg. For a function $f \in C_0(G)$ we can then define the *orbital integral* associated to γ by

$$\mathcal{O}_f(\gamma) = \int_{G/G_\gamma} f(\gamma^{-1} x \gamma)\, dx \tag{A-1}$$

which depends only on the G-conjugacy class $[\gamma]_G$.

AB. *General criterion for Benjamini–Schramm convergence.* Here again X is always a proper Gromov-hyperbolic space and $G = \mathrm{Isom}(X)$. We assume that the action of G on X is nonelementary. The *elliptic radical* of G can then be defined as its unique maximal normal compact subgroup (see [Osin 2017, Proposition 3.4]; in our context, by properness of X bounded elements are the same as compact ones). The following lemma is a special case of [Osin 2017, Theorem 1.5].

Lemma A.3. *Let μ be an invariant random subgroup of G. Then either μ is supported on the elliptic radical or it has full limit set.*

Recall from [Gelander 2019, Section 3] that there is a "Benjamini–Schramm topology" on the set of Borel probability measures on the Gromov–Hausdorff space of pointed proper metric spaces (up to isometry). The set of measures supported on spaces locally isometric to X is precompact in this topology. Moreover, if X is a locally symmetric space then (1-1) is equivalent to $\Gamma_i\backslash X$ converging in the Benjamini–Schramm topology to X.

There is a continuous injective map from the space of invariant random subgroups of G to the Benjamini–Schramm space. If Γ_i are lattices in G then the sequence of uniformly pointed spaces $\Gamma_i\backslash X$ converges to X if and only if the IRSs μ_{Γ_i} converge to the trivial IRS. We will use this to prove the following criterion for convergence, which is a more general version of Proposition 2.1.

Proposition A.4. *Let U the set of hyperbolic isometries in G. Assume that the elliptic radical of G is trivial. If Γ_n is a sequence of lattices in G which satisfies*

$$\lim_{n\to+\infty}\frac{\sum_{[\gamma]_{\Gamma_n}\subset U}\operatorname{vol}((\Gamma_n)_\gamma\backslash G_\gamma)\mathcal{O}_f(\gamma)}{\operatorname{vol}(\Gamma_n\backslash G)}=0 \tag{A-2}$$

then the sequence of metric spaces $\Gamma_n\backslash X$ converges to X in the Benjamini–Schramm topology.

Proof. Let μ_n be the invariant random subgroup of G supported on the conjugacy class of Γ_n. We want to prove that any weak limit μ of a subsequence of (μ_n) is equal to the trivial IRS δ_e. By Lemma A.3 and the fact that a subgroup of G containing no hyperbolic isometries has at most one limit point (see [Gromov 1987, Section 8.2]) it suffices to prove that any such μ contains no hyperbolic isometries.

To prove this choose a covering $U=\bigcup_{C\in\mathcal{C}}C$ of U where $\mathcal{C}$ is countable and every $C\in\mathcal{C}$ is compact. We can do this since Sub_G is metrizable [de la Harpe 2008, Proposition 2]. Let $W_C=\Lambda:\Lambda\cap C\neq\varnothing$; this is a Chabauty-closed subset of Sub_G. If ν is a nontrivial IRS then by Lemma A.3 and previous paragraph it almost surely contains a hyperbolic element. Hence, there is $C\in\mathcal{C}$ such that $\nu(W_C)>0$. We need to prove the opposite for μ, which amounts to the following: for every C there exists a nonnegative Borel function F on Sub_G which is positive on W_C and such that $\int_{\mathrm{Sub}_G}F(\Lambda)\,d\mu(\Lambda)=0$.

Let us fix $C\in\mathcal{C}$ and prove this. There exists an open relatively compact subset V with $C\subset V$ and $\overline{V}\subset U$. Choose any $f\in C^\infty(G)$ such that $f>0$ on C and $f=0$ on $G\setminus V$ and define

$$F(\Lambda)=\begin{cases}\sum_{\lambda\in\Lambda}f(\lambda) & \text{if }\Lambda\text{ is discrete,}\\ 1 & \text{if }\Lambda\text{ is not discrete and intersects }C,\\ 0 & \text{otherwise.}\end{cases}$$

Then F is lower semicontinuous on Sub_G, nonnegative and positive on W_C. On the other hand we have

$$\begin{aligned}\int_{\mathrm{Sub}_G}F(\Lambda)\,d\mu_n(\Lambda)&=\frac{1}{\operatorname{vol}(\Gamma_n\backslash G)}\int_{G/\Gamma_n}\sum_{\gamma\in g\Gamma_n g^{-1}}f(\gamma)\,dg\\&=\frac{1}{\operatorname{vol}(\Gamma_n\backslash G)}\sum_{[\gamma]_{\Gamma_n}\subset U}\operatorname{vol}((\Gamma_n)_\gamma\backslash G_\gamma)\mathcal{O}_\gamma(f).\end{aligned}$$

By the so-called "portemanteau theorem" [Klenke 2014, Theorem 13.16] the limit inferior of the left-hand side is larger or equal to $\int_{\mathrm{Sub}_G} F(\Lambda)\, d\mu(\Lambda)$. By (A-2) we have that the right-hand side converges to 0. It follows that

$$\int_{\mathrm{Sub}_G} F(\Lambda)\, d\mu(\Lambda) = 0$$

which finishes the proof. □

AC. ***Proof of Lemma A.2.*** Let us recall the statement. We have a proper hyperbolic geodesic space X and an hyperbolic isometry γ of X. We fix $x \in X$ and we want to show that there exists constants $C = C(x, \gamma, \delta)$ and $A = A(x, \gamma, \delta)$ such that for any $y \in X$ and any k sufficiently large (depending on γ, x, δ) we have

$$d(y, \gamma^k y) \geq Ck + 2d(y, \langle\gamma\rangle x) - A. \tag{A-3}$$

Let $x, y \in X$. As γ is hyperbolic there exists a, c such that $L = \langle\gamma\rangle x$ is a (c, a)-quasigeodesic. Regarding the conclusion of the proposition it does not change anything if we assume that x is the approximate projection of y on L, meaning that any point x' of L within distance $d(y, L)$ of y, satisfies $d(x', x) \leq K$ (where K depends only on the hyperbolicity constant δ).

Let $\ell = d(x, \gamma x)$. Note first that if k is large enough so that

$$k > 100c\ell^{-1} K \log(k) + ac \tag{A-4}$$

holds, and y is close enough to L so that

$$d(y, x) > c^2 \ell^{-1} \log(k) + cK(2 + \log(2 + k)) + ca \tag{A-5}$$

does not then we see immediately that (A-3) holds, by the triangle inequality. Thus from now on we will assume that both inequalities above hold for y and k.

Let $x_i = \gamma^i x$, $y_i = \gamma^i y$ for $0 \leq i \leq k$. Let F be the finite set

$$F = \{x_0, x_1, \dots, x_k\} \cup \{y_0, y_k\};$$

by [Bowditch 1991, Proposition 7.3.1] there exists a choice of a "spanning tree" on F (that is, a tree whose edges are a subset of all pairs of geodesics segment between points of F) such that

$$\forall p, q \in F : d(p, q) \geq d_{T_F}(p, q) - (1 + \log(2 + k))K \tag{A-6}$$

where K depends only on δ (so we take it equal to the K introduced above to simplify notation). One of y_0, y_k must be connected to one of the x_i in T_F; we may assume that $[y_0, x_i]$ is an edge in T_F for some i. We claim that this i must be unique, and we must have

$$i < c\ell^{-1}((\log(k + 2) + 2)K + a). \tag{A-7}$$

Indeed, let i be the smallest integer such that $[x_i, y_0] \subset T_F$. Then, because

$$d_{T_F}(x_0, y_0) \leq d(x_0, y_0) + (\log(k + 2) + 1)K$$

and

$$d_{T_F}(x_0, y_0) \ge d(x_0, x_i) + d(x_i, y_0) \ge \frac{i\ell}{c} - a + d(x_0, y_0) - K$$

we see that i must verify (A-7). Now assume that there is a $j > i$ such that $[x_j, y_0] \subset T_F$, and take it to be the smallest such; we want to reach a contradiction. Consider $i \le l < j$ to be maximal such that the path in T_F from x_l to x_i does not go through y_0. Then the path in T_F from x_l to x_{l+1} must go through y_0 (otherwise we would have a path from x_{l+1} to x_i via x_l avoiding y_0). We have thus $d_{T_F}(x_l, x_{l+1}) \ge d(x_0, y_0) - K$ which together with (A-5) and (A-6) contradicts the fact that $d(x_l, x_{l+1}) = \ell$.

We now want to prove that $[y_0, y_k]$ is not an edge in T_F. To do so we must consider two possibilities. Assume first that $[y_k, x_j] \subset T_F$ for some j. Then reasoning as above we see that j is the only such index, and $j > k - c\ell^{-1}((\log(k+2)+2)K + a) > i$. In this case we reach a contradiction in the same way as in the previous paragraph: considering a maximal $i \le l < j$ such that the path from x_l to x_i does not go through y_0 we see that $d_{T_F}(x_l, x_{l+1})$ is too large.

If there is no edge $[y_k, x_j]$ in T_F then the path from x_k to y_k must go first to x_i, then to y_0 and finally to y_k. But as $d(x_k, x_i) > (\log(k+2)+1)K$ by (A-7) and (A-4) we see that this contradicts $d(x_0, y_0) = d(x_k, y_k)$.

So we get that there must be a unique edge $[y_k, x_j]$ in T_F, and the path in T_F from y_0 to y_k must go through x_j and x_i. As before we must have

$$j > k - c\ell^{-1}((\log(k+2)+2)K + a)$$

and we finally get using first (A-6), then the fact that $(x_0, \dots, x_k)$ is a quasigeodesic, and finally the above together with (A-7) that:

$$\begin{aligned} d(y_0, y_k) &\ge d(y_0, x_i) + d(x_i, x_j) + d(x_j, y_k) - K - K\log(2+k) \\ &\ge 2d(x_0, y_0) + c^{-1}(j-i)\ell - a - 3K - K\log(2+k) \\ &\ge 2d(x_0, y_0) + c^{-1}\ell k - B - b\log(k) \end{aligned}$$

where B, b depend only on x, γ, δ. From the last inequality and (A-4) we can conclude that (A-3) holds.

Appendix B: Smoothing corners

In this appendix we prove Proposition 3.5; as the argument is technical but has no subtleties we will be quite sketchy in presenting it.

Recall that we have the following situation: X is a manifold with bounded geometry, $H_1, H_2 \subset X$ such that $X \setminus H_i$ both have bounded geometry, meet transversally and the dihedral angle between them is bounded away from 0 and π. We remark that constructing a smoothing of $Y = X \setminus (H_1 \cup H_2)$ satisfying the conclusions of Proposition 3.5 is immediate in the case where the intersection $I = H_1 \cap H_2$ has a neighborhood in Y which is isometric to the product $[0, \delta[^2 \times I$. In general we will prove the following statement: there exists a diffeomorphism φ from $[0, \delta[^2 \times I$ to a neighborhood of I in Y such that φ

and φ^{-1} have all their derivatives uniformly bounded. In view of the preceding remark this proves the proposition.

To define φ we need some more auxiliary notation: for a vector field V and $t \geq 0$ we let Φ_V^t be its flow at time t; if $H \subset Z$ is open with smooth boundary we denote by N_H^Z the normal field of H in Z. We put

$$\varphi_1(x,t,s) = \Phi^t_{N^X_{H_1}}(\Phi^s_{N^{H_1}_I}(x)) \quad \text{and} \quad \varphi_2(x,t,s) = \Phi^s_{N^X_{H_2}}(\Phi^t_{N^{H_2}_I}(x))$$

We fix a smooth nondecreasing function $h : \mathbb{R} \to [0, 1[$ such that h is zero on negative numbers, and at infinity it tends to 1 and all its derivatives vanish at all orders. Let $0 < a < 1$ such that the convex hull of all $\varphi_1(x,t,s)$ and $\varphi_2(x,t,s)$ for $as \leq t \leq a^{-1}s$ is contained in Y. For $x, y \in X$ and $u \in [0,1]$ let $ux + (1-u)y$ denote the barycenter of x, y on the geodesic segment between them.[2] With this notation we define

$$\varphi(x,t,s) = h\left(\frac{at-s}{as-t}\right)\varphi_1(x,t,s) + \left(1 - h\left(\frac{at-s}{as-t}\right)\right)\varphi_2(x,t,s)$$

and we claim that φ has the desired properties. It is smooth as a composition of smooth maps. To deduce the remaining properties we will use the following lemma.

Lemma B.1. *For $i = 1, 2$ there is c depending only on the bounds on the geometry of H_i such that the following properties hold*:

(1) *Let $z \in \partial H_i$ and $0 \leq t \leq \delta$. The linear map $D_z\Phi^t_{N^X_{H_i}}$ is c-Lipschitz on angles. The same holds for $x \in I$ and $D_x\Phi^t_{N^{H_i}_I}$.*

(2) *For all $x \in I$ and all $0 \leq s, t < \delta$, let $y = \Phi^t_{N^X_{H_i}}(\Phi^s_{N^{H_i}_I}(x))$. Let γ be the geodesic (in X) from x to y, u_i the parallel transport along γ of the outward normal vector to H_i at x and $v_i = \frac{\partial}{\partial\tau}\big|_{\tau=t}\Phi^\tau_{N^X_{H_i}}(\Phi^s_{N^{H_i}_I}(x))$. Then the angle between u_i and v_i is at most $c\delta$.*

Proof. (1) follows from the boundedness of coefficients of the metric tensor and its inverse in normal exponential coordinates (in both $I \subset H_i$ and $\partial H_i \subset X$). (2) follows from (1), together with the fact that parallel transport along a closed curve stays close to the identity within the δ-neighborhood. □

Let V_i be the vector fields given by the vectors v_i defined in the lemma. As for any $x \in I$ we have that the angle between $V_1(x)$ and $V_2(x)$ lies in $[\alpha_0, \pi - \alpha_0]$ it follows from (2) that if we choose $\delta < c^{-1}\alpha_0/2$ we have that the angle between V_1 and V_2 at any point x in the δ-neighborhood of I lies in $[\alpha_0/2, \pi - \alpha_0/2]$. In particular V_1, V_2 define a plane field, and we define J to be its orthogonal.

Let π_J be orthogonal projection on J. The block decomposition of $D\varphi$ according to $TX = J \oplus (V_1 + V_2)$ is

$$D_{(x,t,s)}\varphi = \begin{pmatrix} \pi_J D_x\varphi & C \\ (1-\pi_J)D_x\varphi & B \end{pmatrix}.$$

[2] This is well-defined for those pairs of points in X that we consider, as long as we take $\delta \ll \mathrm{inj}(X)$.

We need to prove that:

(1) $D_x\varphi$, B and C have bounded coefficients (in terms of the bounds on the geometry).

(2) $\pi_J D_x\varphi$ and B are everywhere invertible and their inverses are bounded.

(3) $\|(1-\pi_J)D_x\varphi\| \ll \delta$.

Indeed, this shows that the map φ has a derivative which everywhere invertible. In particular, it is a local diffeomorphism and as it is the identity on I it is also a global diffeomorphism. This also implies that its derivative is uniformly bounded in terms of the geometry of H_i and α_0, and so is its inverse.

We deal first with $D_x\varphi$. We note that

$$(D_x\varphi)_{(x,t,s)} = h\left(\frac{at-s}{as-t}\right)D_x\varphi_1(x,t,s) + \left(1-h\left(\frac{at-s}{as-t}\right)\right)D_x\varphi_2(x,t,s) + O(\delta)$$

because of bounded geometry and the fact that to obtain φ we move φ_1 and φ_2 by at most δ. It follows that $D_x\varphi$ is bounded. By point (1) of the lemma we have that at all points the angle between the image of $D_x\varphi$ and V_i is at most $c\delta$; it follows that $\|(1-\pi_J)D_x\varphi\| \ll \delta$. Moreover $D_x\varphi$ is everywhere invertible with bounded inverse, because both $A_1 = D_x\varphi_1$ and $A_2 = D_x\varphi_2$ are, and for $w \in T_xI$ the vectors $A_1(w)$, $A_2(w)$ have an angle $\le c\delta$ between them by (1).

We also have

$$D_t\varphi = h\left(\frac{at-s}{as-t}\right)D_t\varphi_1(x,t,s) + \left(1-h\left(\frac{at-s}{as-t}\right)\right)D_t\varphi_2(x,t,s) + O(\delta)$$

and similarly for $D_s\varphi$, so the coefficients of B, C are bounded.

It remains to prove that B is invertible and $\det(B)$ is bounded away from zero. At a point $x \in I$ we have $D_t\varphi$ and $D_s\varphi$ belong to two disjoint open convex cones in T_xX/J_x; by (2) and (1) this remains true in the δ-neighborhood and the angle between the cones remains bounded away from zero, hence the matrix B is invertible with uniformly bounded inverse.

References

[Abert et al. 2017] M. Abert, N. Bergeron, I. Biringer, T. Gelander, N. Nikolov, J. Raimbault, and I. Samet, "On the growth of L^2-invariants for sequences of lattices in Lie groups", *Ann. of Math.* (2) **185**:3 (2017), 711–790. MR Zbl

[Beardon 1983] A. F. Beardon, *The geometry of discrete groups*, Grad. Texts Math. **91**, Springer, 1983. MR Zbl

[Boileau et al. 2003] M. Boileau, S. Maillot, and J. Porti, *Three-dimensional orbifolds and their geometric structures*, Panoram. Synth. **15**, Soc. Math. France, Paris, 2003. MR Zbl

[Borel and Harish-Chandra 1962] A. Borel and Harish-Chandra, "Arithmetic subgroups of algebraic groups", *Ann. of Math.* (2) **75** (1962), 485–535. MR Zbl

[Bowditch 1991] B. H. Bowditch, "Notes on Gromov's hyperbolicity criterion for path-metric spaces", pp. 64–167 in *Group theory from a geometrical viewpoint* (Trieste, Italy, 1990), edited by É. Ghys et al., World Sci., River Edge, NJ, 1991. MR Zbl

[Bridson and Haefliger 1999] M. R. Bridson and A. Haefliger, *Metric spaces of non-positive curvature*, Grundlehren der Math. Wissenschaften **319**, Springer, 1999. MR Zbl

[Clozel 2003] L. Clozel, "Démonstration de la conjecture τ", *Invent. Math.* **151**:2 (2003), 297–328. MR Zbl

[Elstrodt et al. 1998] J. Elstrodt, F. Grunewald, and J. Mennicke, *Groups acting on hyperbolic space: harmonic analysis and number theory*, Springer, 1998. MR Zbl

[Fenchel 1989] W. Fenchel, *Elementary geometry in hyperbolic space*, de Gruyter Stud. Math. **11**, de Gruyter, Berlin, 1989. MR Zbl

[Fraczyk 2016] M. Fraczyk, "Strong limit multiplicity for arithmetic hyperbolic surfaces and 3-manifolds", preprint, 2016. arXiv

[Gelander 2019] T. Gelander, "A view on invariant random subgroups and lattices", pp. 1321–1344 in *Proc. Int. Congr. Math., I* (Rio de Janeiro, 2018), edited by B. Sirakov et al., World Sci., River Edge, NJ, 2019.

[Gromov 1987] M. Gromov, "Hyperbolic groups", pp. 75–263 in *Essays in group theory*, edited by S. M. Gersten, Math. Sci. Res. Inst. Publ. **8**, Springer, 1987. MR Zbl

[Halpern 1981] N. Halpern, "A proof of the collar lemma", *Bull. Lond. Math. Soc.* **13**:2 (1981), 141–144. MR Zbl

[de la Harpe 2008] P. de la Harpe, "Spaces of closed subgroups of locally compact groups", preprint, 2008. arXiv

[Kazhdan 1977] D. Kazhdan, "Some applications of the Weil representation", *J. Analyse Mat.* **32** (1977), 235–248. MR Zbl

[Klenke 2014] A. Klenke, *Probability theory: a comprehensive course*, 2nd ed., Springer, 2014. MR Zbl

[Levit 2017] A. Levit, "On Benjamini–Schramm limits of congruence subgroups", 2017. To appear in *Israel J. Math.* arXiv

[Li and Millson 1993] J.-S. Li and J. J. Millson, "On the first Betti number of a hyperbolic manifold with an arithmetic fundamental group", *Duke Math. J.* **71**:2 (1993), 365–401. MR Zbl

[Long et al. 2006] D. D. Long, C. Maclachlan, and A. W. Reid, "Arithmetic Fuchsian groups of genus zero", *Pure Appl. Math. Q.* **2**:2 (2006), 569–599. MR Zbl

[Lück 2002] W. Lück, *L^2-invariants: theory and applications to geometry and K-theory*, Ergebnisse der Mathematik (3) **44**, Springer, 2002. MR Zbl

[Lück and Schick 1999] W. Lück and T. Schick, "L^2-torsion of hyperbolic manifolds of finite volume", *Geom. Funct. Anal.* **9**:3 (1999), 518–567. MR Zbl

[Matz 2019] J. Matz, "Limit multiplicities for $\mathrm{SL}_2(\mathbb{O}_F)$ in $\mathrm{SL}_2(\mathbb{R}^{r_1} \oplus \mathbb{C}^{r_2})$", *Groups Geom. Dyn.* **13**:3 (2019), 841–881. MR

[Millson 1976] J. J. Millson, "On the first Betti number of a constant negatively curved manifold", *Ann. of Math.* (2) **104**:2 (1976), 235–247. MR Zbl

[Osin 2017] D. Osin, "Invariant random subgroups of groups acting on hyperbolic spaces", *Proc. Amer. Math. Soc.* **145**:8 (2017), 3279–3288. MR Zbl

[Raimbault 2017] J. Raimbault, "On the convergence of arithmetic orbifolds", *Ann. Inst. Fourier* (*Grenoble*) **67**:6 (2017), 2547–2596. MR Zbl

[Shimura 1971] G. Shimura, *Introduction to the arithmetic theory of automorphic functions*, Kanô Memor. Lect. **1**, Iwanami Shoten, Tokyo, 1971. MR Zbl

[Taylor 2011] M. E. Taylor, *Partial differential equations, I: Basic theory*, 2nd ed., Appl. Math. Sci. **115**, Springer, 2011. MR Zbl

[Thompson 1980] J. G. Thompson, "A finiteness theorem for subgroups of PSL(2, $\mathbb{R}$) which are commensurable with PSL(2, $\mathbb{Z}$)", pp. 533–555 in *Santa Cruz Conf. Finite Groups* (Santa Cruz, CA, 1979), edited by B. Cooperstein and G. Mason, Proc. Sympos. Pure Math. **37**, Amer. Math. Soc., Providence, RI, 1980. MR Zbl

[Zograf 1991] P. Zograf, "A spectral proof of Rademacher's conjecture for congruence subgroups of the modular group", *J. Reine Angew. Math.* **414** (1991), 113–116. MR Zbl

Communicated by Peter Sarnak
Received 2018-11-30 Revised 2019-04-19 Accepted 2019-08-15

fraczyk@renyi.hu *Alfréd Rényi Institute of Mathematics, Budapest, Hungary*

jean.raimbault@math.univ-toulouse.fr *Institut de Mathématiques de Toulouse, Université de Toulouse, CNRS, UPS IMT, France*

ALGEBRA AND NUMBER THEORY 13:10 (2019)
dx.doi.org/10.2140/ant.2019.13.2383

Combinatorial identities and Titchmarsh's divisor problem for multiplicative functions

Sary Drappeau and Berke Topacogullari

Given a multiplicative function f which is periodic over the primes, we obtain a full asymptotic expansion for the shifted convolution sum $\sum_{|h|<n\leq x} f(n)\tau(n-h)$, where τ denotes the divisor function and $h\in\mathbb{Z}\setminus\{0\}$. We consider in particular the special cases where f is the generalized divisor function τ_z with $z\in\mathbb{C}$, and the characteristic function of sums of two squares (or more generally, ideal norms of abelian extensions). As another application, we deduce a full asymptotic expansion in the generalized Titchmarsh divisor problem $\sum_{|h|<n\leq x,\,\omega(n)=k} \tau(n-h)$, where $\omega(n)$ counts the number of distinct prime divisors of n, thus extending a result of Fouvry and Bombieri, Friedlander and Iwaniec.

We present two different proofs: The first relies on an effective combinatorial formula of Heath-Brown's type for the divisor function τ_α with $\alpha\in\mathbb{Q}$, and an interpolation argument in the z-variable for weighted mean values of τ_z. The second is based on an identity of Linnik type for τ_z and the well-factorability of friable numbers.

1. Introduction

Understanding correlations of arithmetic functions is a fundamental question in analytic number theory. In an explicit form, the problem can be stated as determining the asymptotic behavior of the sum

$$\sum_{1<n\leq x} f(n)g(n-1), \tag{1-1}$$

where $f, g:\mathbb{N}\to\mathbb{C}$ are arithmetic functions of multiplicative nature. Many important problems in number theory can be rephrased in terms of correlations of arithmetic functions, the twin prime conjecture or the Goldbach conjecture being two famous examples (see e.g., [Elliott 1994, Chapter 1]). Sums of the form (1-1) also come up prominently in the study of growth properties of L-functions in the critical strip. In this context, the problem is known as the shifted convolution problem and has a long and rich history (see [Michel 2007] for an overview).

In general, determining the precise asymptotic behavior of the unweighted correlation (1-1) is a difficult task and only very few unconditional results are known in this direction, all of them requiring at least one

We thank O. Ramaré, H. L. Montgomery, R. C. Vaughan, R. de la Bretèche, É. Fouvry, G. Tenenbaum and the anonymous referee for helpful discussions and remarks on the present work. In particular we thank É. Fouvry and G. Tenenbaum for remarks which led to the second proof presented here. Part of this work was done during a visit of BT to Aix-Marseille university, supported by the French-Austrian joint project MuDeRa (FWF I-1751-N26, ANR-14-CE34-0009).
MSC2010: primary 11N37; secondary 11N25.
Keywords: shifted convolution, divisor function, combinatorial identity.

of the involved functions to be very close — in the convolution sense — to the constant function **1**, the divisor function $\tau(n)$ or to Fourier coefficients of GL_2-automorphic forms. Note that when f and g are bounded, the *logarithmically* weighted correlation

$$\sum_{1<n\leq x} \frac{f(n)g(n-1)}{n}$$

has been the object of a recent breakthrough of Tao [2016]. The case of higher-order correlations of bounded functions with logarithmic weight was also recently settled in [Tao and Teräväinen 2019].

In the present paper, we focus on the particularly important case $g(n) = \tau(n)$ of the unweighted problem (1-1), which is at the edge of current techniques. If the average value of f is not too small, it was already observed by Vinogradov [1965] (in the case of primes; see also [Rodriquez 1965; Halberstam 1967]) that simple asymptotic equivalences for the sum

$$\sum_{1<n\leq x} f(n)\tau(n-1) \tag{1-2}$$

can be obtained from analogues of the Bombieri–Vinogradov and Brun–Titchmarsh inequalities. We refer to [Green 2018; Granville and Shao 2018; Fouvry and Radziwiłł 2018] for recent works on this topic. In particular, Corollary 1.3 in [Fouvry and Radziwiłł 2018] leads to a partial asymptotic formula for (1-2) (including all terms with nonnegative exponent of $\log x$) for a large set of arithmetic functions f, including the generalized divisor function τ_z which we discuss further below.

It is a considerably more difficult problem to obtain full asymptotic expansions for (1-2), say, with an error term of the form $\mathcal{O}(x(\log x)^{-N})$ where $N > 0$ is fixed but can be chosen arbitrarily large. The gap in difficulty is related to the "$x^{1/2}$"-barrier for primes in arithmetic progressions on average over moduli. To our knowledge full asymptotic expansions are known for only very few specific examples of functions f of arithmetic interest:

- The indicator function of primes [Fouvry 1985; Bombieri et al. 1986].
- The indicator function of integers without large prime factors [Fouvry and Tenenbaum 1990; Drappeau 2015].
- The k-fold divisor functions $\tau_k(n)$, $k \in \mathbb{N}$, $k \geq 2$ [Motohashi 1980; Topacogullari 2016; 2018].

The methods from the last example can also be used to handle the case where f is given by Fourier coefficients of GL_2-automorphic forms, although this does not seem to be worked out explicitly in the literature.

The purpose of the present paper is to introduce two new methods which lead to an asymptotic expansion for (1-2) for a wide class of multiplicative functions. Let $A, D \geq 1$ be fixed integers. Define $\mathcal{F}_D(A)$ to be the set of all multiplicative functions $f : \mathbb{N} \to \mathbb{C}$ which are D-periodic over the primes in the sense that

$$f(p_1) = f(p_2) \quad \text{for any primes } p_1 \text{ and } p_2 \text{ with } p_1 \equiv p_2 \bmod D,$$

and which satisfy the growth condition,

$$|f(n)| \leq \tau_A(n) \quad \text{for all } n \in \mathbb{N},$$

where $\tau_A(n)$ denotes the generalized divisor function. Our main result is the following preliminary asymptotic formula for the sum (1-2) for $f \in \mathcal{F}_D(A)$.

Theorem 1.1. *Let $A, D, N \geq 1$. For all $f \in \mathcal{F}_D(A)$ and all $x \geq 2$, we have*

$$\sum_{1<n\leq x} f(n)\tau(n-1) = 2 \sum_{\substack{\chi \text{ primitive} \\ \operatorname{cond}(\chi)\,|\,D}} \sum_{\substack{q\leq\sqrt{x} \\ \operatorname{cond}(\chi)\,|\,q}} \frac{1}{\varphi(q)} \sum_{\substack{q^2\leq n\leq x \\ (n,q)=1}} f(n)\chi(n) + \mathcal{O}\biggl(\frac{x}{(\log x)^N}\biggr), \tag{1-3}$$

where the implied constant depends only on A, D and N.

Remarks. • The main term in (1-3) can be evaluated asymptotically by classical methods, for instance the Selberg–Delange method [Tenenbaum 1995, Chapter II.5]. The ensuing expression will in general take the form

$$x \sum_{\kappa\in K_f} (\log x)^{\kappa} \sum_{\ell=0}^{N} \frac{c_{\kappa,\ell}}{(\log x)^{\ell}} + O\biggl(\frac{x}{(\log x)^{N-\max(K_f)+1}}\biggr), \tag{1-4}$$

for some finite set $K_f \subset \mathbb{C}$ and some sequences $(c_{\kappa,\ell})_{\ell=0}^{N}$ of complex numbers. We spell this out in detail in three particular cases below.

• If f satisfies a Siegel–Walfisz estimate in the sense that

$$\sum_{n\leq x} f(n)\chi(n) = O_A(x(\log x)^{-A}),$$

uniformly for all primitive characters of conductor $1 < q \leq (\log x)^A$, then only the trivial character contributes to the main term in (1-3), and the formula simplifies to

$$\sum_{1<n\leq x} f(n)\tau(n-1) = 2 \sum_{q\leq\sqrt{x}} \frac{1}{\varphi(q)} \sum_{\substack{q^2\leq n\leq x \\ (n,q)=1}} f(n) + \mathcal{O}\biggl(\frac{x}{(\log x)^N}\biggr).$$

For the main term one then has an expansion as in (1-4) with $K_f = \{\kappa_f\}$, where κ_f is the average value of $f(p)$ over all primes p.

• We stress that the implied constant is uniform in all $f \in \mathcal{F}_D(A)$, and depends only on A, D and N. This feature can be useful in applications (see Section 1C).

• On the other hand, our result is badly behaved with respect to D, partly due to the use of the Siegel–Walfisz theorem. The arguments presented here do not seem sufficient to obtain an improvement in this aspect, although this does not affect our applications.

• The error term in (1-3) corresponds to an application of the Siegel–Walfisz theorem. If the Riemann hypothesis is true for all Dirichlet L-functions, then it can be improved to $\mathcal{O}(x^{1-\delta})$ for some absolute constant $\delta > 0$.

Theorem 1.1 may also be interpreted as a result of Bombieri–Vinogradov type "beyond $\sqrt{x}$" for the average of $f \in \mathcal{F}_D(A)$ in the residue classes of a fixed integer and without absolute values. By a slight modification of the method presented here, it is possible to show that for $f \in \mathcal{F}_D(A)$,

$$\sum_{q \le \sqrt{x}} \Biggl(\sum_{\substack{1<n\le x \\ n\equiv 1 \bmod q}} f(n) - \frac{1}{\varphi(q)} \sum_{\substack{\chi \text{ primitive} \\ \operatorname{cond}(\chi) \mid (D,q)}} \sum_{\substack{1<n\le x \\ (n,q)=1}} f(n)\chi(n) \Biggr) = \mathcal{O}_{A,D,N}\biggl(\frac{x}{(\log x)^N} \biggr).$$

We refer to [Green 2018; Granville and Shao 2018] for recent works related to this point of view.

In many applications correlation sums with more general shifts appear and it is important to have results which are uniform in large ranges of the involved parameters. Our methods are robust enough to be applied to these cases as well, and Theorem 1.1 is in fact the special case $a = h = 1$ of the following more general result.

Theorem 1.2 (general shifts). *Let A, D, $N \ge 1$. There exists an absolute constant $\delta > 0$, such that, for all $f \in \mathcal{F}_D(A)$, all $x \ge 2$ and all $a, h \in \mathbb{Z}$ satisfying $1 \le a, |h| \le x^\delta$, we have*

$$\sum_{|h|/a < n \le x} f(n)\tau(an-h) = M_f(x; h, a) + \mathcal{O}\biggl(\tau((a,h)) \frac{x}{(\log x)^N} \biggr),$$

where $M_f(x; a, h)$ is given by

$$M_f(x; a, h) := 2 \sum_{\substack{\chi \text{ primitive} \\ \operatorname{cond}(\chi) \mid D}} \sum_{\substack{q \le \sqrt{ax} \\ \operatorname{cond}(\chi) \mid \frac{q}{(q,h)}}} \frac{\bar{\chi}\bigl(\frac{h}{(h,q)}\bigr)}{\varphi\bigl(\frac{q}{(h,q)}\bigr)} \sum_{\substack{q^2/a \le n \le x \\ (an,q)=(h,q)}} f(n)\chi\bigl(\tfrac{an}{(an,q)}\bigr),$$

and where the implied constant depends only on A, D and N.

Unfortunately, the range of uniformity in h in Theorem 1.2 is comparatively short. This is due to a known uniformity issue of arguments based on exponential sums estimates underlying our bilinear sums estimate (see [Fouvry and Iwaniec 1983, page 200]). Out of the same reason, the methods used here are not able to address the dual problem

$$\sum_{n=1}^{N-1} f(n)\tau(N-n)$$

(for which results are available for instance when $f = \tau$ or $f = \tau_3$, see [Motohashi 1994; Topacogullari 2016]).

We mention that results are known for affine correlations whose linear parts are pairwise independent [Matthiesen 2012; 2016], or when there is an additional, long enough average over the shift [Mikawa 1992; Matomäki et al. 2019a; 2019b]. See also [Andrade et al. 2015; Bary-Soroker and Fehm 2019] for a function field analogue in the large q limit.

Finally, we mention the work of Pitt [2013]. He considered an analogue of the Titchmarsh divisor problem (see Section 1C) with the divisor function replaced by Fourier coefficients of holomorphic cusp forms. In many situations, these Fourier coefficients and the divisor function exhibit a similar behavior, since the latter can also be viewed as the Fourier coefficients of an Eisenstein series (see e.g., [Iwaniec 2002, Chapter 3.4]). Remarkably, Pitt obtained an estimate with a power saving in the error term unconditionally, something which is not known for the original Titchmarsh divisor problem. It seems possible that his ideas can be adapted to our setting, and that one might obtain an analogue of Theorem 1.2 with the divisor function replaced by Fourier coefficients of holomorphic cusp forms and with a power saving in the error term. We do not pursue this here.

We apply Theorem 1.2 to three functions f of particular arithmetic interest:

(1) The generalized divisor functions $\tau_z(n)$ with $z \in \mathbb{C}$.

(2) The indicator function of integers n which are norms of an integral ideal in an abelian extension.

(3) The indicator function of integers n with exactly k different prime factors.

1A. ***Correlations of divisor functions.*** Our first application is related to the generalized additive divisor problem, which asks for an asymptotic evaluation of

$$D_{k,\ell}(x,h) := \sum_{|h|<n\le x} \tau_k(n)\tau_\ell(n+h)$$

for integers $k, \ell \ge 2$. This problem has received a lot of attention, partly motivated by its connection to the $2k$-th moment of the Riemann zeta function (see [Ivić 1991, Chapter 4] or [Conrey and Keating 2016; Ng and Thom 2019]).

It is conjectured that for some constant $C_{k,\ell}(h) > 0$,

$$D_{k,\ell}(x,h) \sim C_{k,\ell}(h)x(\log x)^{k+\ell-2},$$

and it is known [Henriot 2012] that this is the correct order of magnitude. However, this has been proven only for the cases where either $k = 2$ or $\ell = 2$. In these cases, the best-known results in the literature are of the form

$$D_{k,2}(x,h) = x P_{k,h}(\log x) + \mathcal{O}(x^{\theta_k+\varepsilon}) \quad \text{for} \quad h \ll x^{\eta_k},$$

where $P_{k,h}$ is a degree k polynomial depending on h, with:

- $\theta_2 = \frac{2}{3}$ and $\eta_2 = \frac{2}{3}$ [Deshouillers and Iwaniec 1982a; Motohashi 1994].
- $\theta_3 = \frac{8}{9}$ and $\eta_3 = \frac{2}{3}$ [Friedlander and Iwaniec 1985; Topacogullari 2016].
- $\theta_k = \max\bigl(1 - \frac{4}{15k-9}, \frac{56}{57}\bigr)$ and $\eta_k = \frac{15}{19}$ ($k \ge 4$ fixed) [Linnik 1963; Fouvry and Tenenbaum 1985; Topacogullari 2018].

In the case $k = \ell = 2$, a similar asymptotic formula holds in a much larger range of uniformity for h, although with a weaker error term (see [Meurman 2001] for the currently best results in this direction). For $k, \ell \ge 3$ the problem remains completely open.

The functions τ_k are special cases of coefficients of the Dirichlet series

$$\sum_{n=1}^{\infty} \frac{\tau_z(n)}{n^s} := \zeta(s)^z \quad \text{for } z \in \mathbb{C} \text{ and } \mathfrak{Re}(s) > 1.$$

On prime powers, they are given explicitly by

$$\tau_z(p^\ell) = \binom{z+\ell-1}{\ell}. \tag{1-5}$$

The functions τ_z for $z \notin \mathbb{N}$ have a more complicated behavior than those for $z \in \mathbb{N}$. When $z = -1$ for instance, we recover the Möbius function $\tau_{-1}(n) = \mu(n)$.

Theorem 1.2 leads to an asymptotic expansion of $D_{z,2}(x, h)$ for arbitrary $z \in \mathbb{C}$, uniformly in any fixed disk $|z| \ll 1$.

Theorem 1.3. *Let $A, N \geq 1$ and $\varepsilon > 0$. There exist a constant $\delta > 0$ and holomorphic functions $\lambda_{h,\ell} : \mathbb{C} \to \mathbb{C}$, such that, for $|z| \leq A$, $x \geq 2$ and $1 \leq |h| \leq x^\delta$,*

$$\sum_{|h|<n\leq x} \tau_z(n)\tau(n+h) = x(\log x)^z \sum_{\ell=0}^{N} \frac{\lambda_{h,\ell}(z)}{(\log x)^\ell} + \mathcal{O}\biggl(\frac{x(\log x)^{\mathfrak{Re}(z)}}{(\log x)^{N+1-\varepsilon}}\biggr), \tag{1-6}$$

where the implicit constant only depends on A, N and ε.

The coefficients $\lambda_{h,\ell}(z)$ can be computed explicitly; see (8-4) infra for an expression of the leading coefficient. If z is a nonpositive integer, all the coefficients $\lambda_{h,\ell}(z)$ vanish and (1-6) effectively becomes an upper bound.

Our method leads to a power saving error term in Theorem 1.3 when $z = k \in \mathbb{N}$. This is solely due to the fact that in these cases the k-th power of Dirichlet L-functions $L(s, \chi)^k$ can be continued analytically to a strip $\mathfrak{Re}(s) \geq 1 - \delta$ for some $\delta > 0$ (excluding the possible pole at $s = 1$). We do not focus of the case $z \in \mathbb{N}$ here, since the works mentioned above then give quantitatively stronger estimates.

1B. ***Norms of integral ideals.*** Let $K/\mathbb{Q}$ be a Galois extension with discriminant Δ_K. We define

$$\mathcal{N}_K := \{N(\alpha) : \alpha \text{ ideal of } \mathcal{O}_K, \alpha \neq 0\}.$$

This set has a rich multiplicative structure, described by the Artin reciprocity law. When the extension is abelian, the Dedekind function $\zeta_K(s)$ factorizes into Dirichlet L-functions mod Δ_K, so that the integers in $\mathcal{N}_K$ can be detected by looking at the congruence classes of their prime factors mod Δ_K. Theorem 1.2 eventually applies and leads to the following result.

Theorem 1.4. *Let $K/\mathbb{Q}$ be an abelian field extension. Let $N \geq 1$ and $\varepsilon > 0$. There exist a constant $\delta > 0$ and real numbers $\kappa_{h,\ell}(K)$, such that, for $x \geq 2$ and $1 \leq |h| \leq x^\delta$,*

$$\sum_{\substack{|h|<n\leq x \\ n\in\mathcal{N}_K}} \tau(n-h) = x(\log x)^{1-1/[K:\mathbb{Q}]} \sum_{\ell=0}^{N} \frac{\kappa_{h,\ell}(K)}{(\log x)^\ell} + \mathcal{O}\biggl(\frac{x}{(\log x)^{N+1/[K:\mathbb{Q}]-\varepsilon}}\biggr), \tag{1-7}$$

where the implicit constant depends only on K, N and ε.

An interesting special case is given by the extension $\mathbb{Q}(i)/\mathbb{Q}$. In this case, $\mathcal{N}_{\mathbb{Q}(i)}$ is simply the set of integers which can be written as a sum of two squares, and Theorem 1.4 takes the following form.

Corollary 1.5. *Let $\mathcal{B}$ be the set of all integers which can be written as a sum of two squares. Let $N \geq 1$ and $\varepsilon > 0$. There exist a constant $\delta > 0$ and real numbers $\beta_{h,\ell}$, such that, for $x \geq 2$ and $1 \leq |h| \leq x^\delta$,*

$$\sum_{\substack{|h|<n\leq x \\ n\in\mathcal{B}}} \tau(n-h) = x(\log x)^{1/2} \sum_{\ell=0}^{N} \frac{\beta_{h,\ell}}{(\log x)^\ell} + \mathcal{O}\left(\frac{x}{(\log x)^{N+1/2-\varepsilon}}\right). \tag{1-8}$$

where the implicit constant depends only on N and ε.

The first term in the asymptotic formula for the left-hand side of (1-8) can also be obtained using a recent extension of the Bombieri–Vinogradov theorem due to Granville and Shao [2018], along with the Brun–Titchmarsh inequality. The coefficients $\kappa_{h,\ell}(K)$ and $\beta_{h,\ell}$ can be computed explicitly; see (8-5) infra for an evaluation of the leading coefficient $\beta_{h,0}$ in (1-8). Note that, since the indicator function $b(n)$ of the set $\mathcal{B}$ correlates with both the principal and the nonprincipal character mod 4, there are two genuine contributions on the right-hand side in (1-3) when $f(n) = b(n)$. This also explains the discrepancy between the conjectures made in [Iwaniec 1976] and [Freiberg et al. 2017] on autocorrelations of $b(n)$.

We stress that the multiplicity of representations as ideal norms in Corollary 1.5 is *not* taken into account. Thus the estimate (1-8) is more difficult to obtain than an estimate for the correlation sum

$$\sum_{|h|<n\leq x} r_2(n)\tau(n-h) \quad \text{with } r_2(n) := |\{(r,s)\in\mathbb{Z}^2 : r^2+s^2=n\}|,$$

for which classical methods suffice.

1C. *Integers with k prime divisors.* The Titchmarsh divisor problem [1930] asks for an asymptotic evaluation of the sum

$$\sum_{|h|<p\leq x} \tau(p-h), \tag{1-9}$$

where p runs over all primes up to x. Following the initial works by Titchmarsh [1930] and Linnik [1963], the best known result was obtained independently by Fouvry [1985] and Bombieri, Friedlander and Iwaniec [Bombieri et al. 1986]: For any fixed $N > 0$, we have, for $1 \leq |h| \leq (\log x)^N$,

$$\sum_{|h|<p\leq x} \tau(p-h) = C_h x + C_h' \operatorname{li}(x) + \mathcal{O}\left(\frac{x}{(\log x)^N}\right), \tag{1-10}$$

where

$$C_h = \frac{\zeta(2)\zeta(3)}{\zeta(6)} \prod_{p\mid h}\left(1 - \frac{p}{p^2-p+1}\right), \quad C_h' = \left(\gamma - \sum_p \frac{\log p}{p^2-p+1} + \sum_{p\mid h} \frac{p^2\log p}{(p-1)(p^2-p+1)}\right) C_h.$$

An interesting generalization of this problem concerns the sum

$$\sum_{\substack{|h|<n\leq x\\ \omega(n)=k}} \tau(n-h), \tag{1-11}$$

where $\omega(n)$ denotes the number of distinct prime divisors of an integer n. An asymptotic equivalence for this sum was proven by Khripunova [1998, Theorem 3], uniformly for $k \ll \log\log x$ and $h \ll x$.

Our methods allow to obtain a full asymptotic expansion for (1-11), at least for small shifts h. In order to circumvent the obstacle that the indicator function for integers n with $\omega(n) = k$ is not multiplicative, we use a classical method due to Selberg [1954], which allows us to reduce the evaluation of (1-11) to the evaluation of the correlation sum of the divisor function with the multiplicative function $n \mapsto z^{\omega(n)}$. This eventually leads to the following result.

Theorem 1.6. *Let $N \geq 1$ and $\varepsilon > 0$. There exist a constant $\delta > 0$ and polynomials $P^k_{h,\ell}(X)$ of degree $k-1$ such that, for $1 \leq k \ll \log\log x$ and $|h| \leq x^\delta$,*

$$\sum_{\substack{|h|<n\leq x\\ \omega(n)=k}} \tau(n-h) = x \sum_{0\leq \ell\leq N} \frac{P^k_{h,\ell}(\log\log x)}{(\log x)^\ell} + \mathcal{O}\left(\frac{x(\log\log x)^k}{k!(\log x)^{N+1-\varepsilon}}\right), \tag{1-12}$$

where the implicit constants depend only on N and ε.

The case $k = 1$ recovers the best-known asymptotic formula (1-10) for the Titchmarsh divisor problem. As before, the polynomials $P^k_{h,\ell}$ can be computed explicitly; in particular, the leading coefficient in the asymptotic expansion is given by $C_h/(k-1)!$.

This result is nontrivial throughout the range $k \ll \log\log x$. The case $k/\log\log x \to +\infty$ is an interesting question which would require different tools, due to the sparsity of the set of integers under consideration (not unlike the situation for friable integers [Harper 2012]). We do not address this here.

1D. ***Overview of the proof of Theorem 1.2.*** For the sake of clear exposition, we will focus here on the case $D = 1$, as our arguments extend without much difficulty to the case of general moduli and the arising complications are mainly of technical nature. Note that any $f \in \mathcal{F}_1(A)$ can be approximated (in the convolution sense) by a suitable generalized divisor function, so that it suffices to consider the case $f = \tau_z$ with $z \in \mathbb{C}$.

We will give two distinct proofs of Theorem 1.2. They are based on two different kinds of combinatorial identities for the generalized divisor function τ_z, both of which we believe are of independent interest. Our first approach relies on an effective combinatorial formula of Heath-Brown's type for the divisor function τ_α with $\alpha \in \mathbb{Q}$, and an interpolation argument in the z-variable for weighted mean values of τ_z. Our second approach, which is more direct and avoids the interpolation step, is instead based on an identity of Linnik type for τ_z and the well-factorability of friable numbers[1].

[1] The second proof was found only after a preliminary version of the present manuscript was uploaded online.

1D.1. *Proof by Heath-Brown's identity and interpolation.* Our first proof of Theorem 1.2 divides into two parts: We first prove the theorem for rational z, and then extend this result to all $z \in \mathbb{C}$.

For $z \in \mathbb{Q}$, the general structure of the proof of Theorem 1.2 follows the setup of [Fouvry 1985; Bombieri et al. 1986] (see also [Fouvry 1984]). The strategy naturally splits into two steps:

(1) We decompose the function f into convolutions with either large smooth components (type I) or suitably localized components (type II).

(2) We solve the question for both types of sums.

The bulk of the present work concerns the first step. Combinatorial decompositions for prime numbers have a long history since the works of Vinogradov [1937] (we refer to the survey [Ramaré 2013] for an account and further references). Yet, it was not until recently that analogous identities emerged for generalized divisor functions. Montgomery and Vaughan (private communication) have recently developed a combinatorial identity of Vaughan's type [1975] for $\tau_{1/2}$, which initially motivated largely the present work. Unfortunately, as for primes, the bilinear sums coming from a raw application of this identity are not quite localized enough to be effective for Titchmarsh's problem, and even though this can sometimes be fixed by iterating the formula [Fouvry 1981], our early attempts were unsuccessful. Instead we follow the more flexible approach of Heath-Brown [1982] (which is related to [Gallagher 1968]).

Our first result (Theorem 3.2 below) is a uniform combinatorial formula of Heath-Brown's type for the divisor function $\tau_{\frac{u}{v}}$ with $u/v \in \mathbb{Q}$. In the simplest case $0 < u < v$, it reads

$$\tau_{u/v}(n) = \sum_{\ell=1}^{K} c_{\ell,K,u/v} \mathop{\sum \cdots \sum}_{\substack{m_1 \cdots m_\ell n_1 \cdots n_{\ell v-u} = n \\ n_1,\dots,n_{\ell v-u} \le x^{1/K}}} \tau_{-1/v}(n_1) \cdots \tau_{-1/v}(n_{\ell v-u}) \quad \text{for } n \le x, \tag{1-13}$$

where $K \in \mathbb{N}_{>0}$ is arbitrary and where $c_{\ell,K,u/v} \in \mathbb{Q}$. A more general formula holds for any rational number u/v (see Theorem 3.2). A crucial property of this formula is that it is sensitive almost only to the archimedean size of u/v. Indeed, for $|u/v| \le A$, the coefficients $c_{\ell,K,u/v}$, the length of the ℓ-sum and the value at primes $n = p$ of each ℓ-summand on the right-hand side are bounded in terms of A and K only (but not of v). Thus, the only loss due to the size of v comes from the number $\mathcal{O}(v)$ of terms in the convolution, which has essentially no effect on what follows.

In the same way, we can express any rational convolution power $*^{u/v} f$ of a multiplicative function in terms of higher convolutions $*^k f$ with $1 \le k \le K$ and a bilinear term with one component supported on the interval $[x^\varepsilon, x^{1/K}]$. However, to our knowledge asymptotic formulae for the correlation sums

$$\sum_{n \le x} (*^k f)(n) \tau(n+1), \tag{1-14}$$

for $k \ge 2$ are currently known for only very few functions f (essentially constant functions and Dirichlet characters). This is the main obstacle towards using decompositions of this form to prove Theorem 1.2 for complex-fold convolutions of multiplicative functions.

Regarding the second step, we are mostly able to use the harmonic analysis arguments underlying [Fouvry 1985; Bombieri et al. 1986]. They are based on bounds on Kloosterman sums on average [Deshouillers and Iwaniec 1982b], along with Voronoi summation (for type I) and Linnik's dispersion method (for type II). We will follow the treatment made in [Drappeau 2017; Topacogullari 2018], although some work is needed in order to cast the main terms from these works in a form suitable for us.

Eventually, the arguments described above yield a proof of Theorem 1.2 for $f = \tau_{\frac{u}{v}}$ uniformly in the range $v \leq (\log x)^N$. As it turns out, this is already sufficient information to be able to conclude.

To see why, we return to the correlation sum

$$D(z) := \sum_{|h|/a < n \leq x} \tau_z(n)\tau(an-h)$$

with $z \in \mathbb{C}$, $|z| \ll 1$. The main observation is that this expression is a polynomial in z, and that we know how to evaluate it on rational numbers with small denominators. Even though $D(z)$ initially has degree of the order of $\log x$, we can use large deviation bounds on the function $\omega(n)$ (and a convolution argument) to approximate it, up to an admissible error, by the polynomial

$$\tilde{D}(z) := \sum_{\substack{|h|/a < n \leq x \\ \omega(n) \ll \log\log x}} z^{\omega(n)}\tau(an-h),$$

which has degree at most $\mathcal{O}(\log\log x)$. This enables us to use Lagrange interpolation on a suitably chosen set of rational sample points to transfer our estimates for $z \in \mathbb{Q}$ to estimates of the same quality for $z \in \mathbb{C}$. Indeed, this process introduces an error which grows exponentially in the degree of the polynomial. As our estimates for $D(z)$ for $z \in \mathbb{Q}$ save an arbitrarily large power of $\log x$, we are still able to obtain an asymptotic formula at the end.

Note that for the above arguments to work it is crucial that estimates with a saving of a large power of $\log x$ for $D(z)$ for $z \in \mathbb{Q}$ are available, which we can fortunately obtain here from the Siegel–Walfisz bound (an unfortunate consequence of the last fact, however, is that most of our results are not effective).

We mention that, as in Heath-Brown's work [1982], the arguments sketched above can be used to obtain asymptotic formulae for short sums

$$\sum_{x < n \leq x+y} f(n)$$

for $y \geq x^{7/12+\varepsilon}$ and $f \in \mathcal{F}_D(A)$, as well as theorems of Bombieri–Vinogradov type. However, unlike Titchmarsh's divisor problem, such results could in principle also be obtained by zero-density estimates for Dirichlet L-functions (see [Iwaniec and Kowalski 2004, Chapter 10.5; Bombieri 1965]).

1D.2. *Proof by Linnik's identity.* Our second proof uses a different decomposition for τ_z, which has the major advantage that it holds uniformly for all z in a fixed bounded subset of $\mathbb{C}$. This avoids the interpolation step necessary in the first proof, although the resulting combinatorial identity is not as elegant as the identity of Heath-Brown's type described above.

A naive attempt to find a combinatorial formula for τ_z which is uniform in z might start with Linnik's formula [Iwaniec and Kowalski 2004, Section 13.3], which relies on the Taylor series expansion

$$\zeta(s)^z = (1+(\zeta(s)-1))^z = \sum_{j\geq 0}\binom{z}{j}(\zeta(s)-1)^j.$$

The main technical difficulty at this point is to truncate the sum over j. In the context of Linnik's formula, this truncation is performed by restricting to almost-primes from the outset (or inserting a sieve weight), see [Linnik 1963, page 21], but unfortunately this approach is not available in our situation.

Instead we write $\zeta(s) = \zeta_y(s)M_y(s)$, where

$$\zeta_y(s) := \prod_{p\leq y}\left(1-\frac{1}{p^s}\right)^{-1} \quad \text{and} \quad M_y(s) := \frac{\zeta(s)}{\zeta_y(s)},$$

with $y = x^{1/K}$ for some $K \in \mathbb{N}$, and then apply the Taylor series expansion only on the second factor $M_y(s)$, so that

$$\zeta(s)^z = \zeta_y(s)^z \sum_{j\geq 0}\binom{z}{j}(M_y(s)-1)^j.$$

This expression has the advantage that the j-th summand has no coefficient for $n \leq y^j$ in its Dirichlet series expansion. After expanding and comparing the Dirichlet coefficients on both sides, we are therefore led to the following "raw" combinatorial decomposition (see Theorem 3.3),

$$\tau_z(n) = \sum_{0\leq \ell < K} c_\ell \sum_{\substack{n=n_1n_2 \\ n_1 \text{ is } y\text{-friable}}} \tau_{z-\ell}(n_1)\tau_\ell(n_2) \quad \text{for } n \leq x,$$

where the c_ℓ are some complex numbers which depend on z, but which can be bound uniformly for $z \ll 1$ (we recall that an integer is said to be y-friable if all of its prime factors are bounded by y).

In order to apply this formula, it is of course necessary to be able to control the factors $\tau_{z-\ell}(n_1)$. However, the characteristic function of y-friable numbers has good factorability properties (see [Vaughan 1989, page 66; Fouvry and Tenenbaum 1996, Lemme 3.1]): we can essentially replace them in the formula above by convolutions of sequences supported on $[1, y]$ (see Lemma 3.4). This in turn enables us to apply estimates of type I and type II, leading eventually to the desired asymptotic formula.

Plan. In Section 2, we introduce our main notations and the subsets of functions of $\mathcal{F}_D(A)$ we will mainly work with. In Section 3, we present the combinatorial decompositions for τ_z, on which our proofs are based. In Section 4, we state some auxiliary computations in order to use the results of [Topacogullari 2018; Drappeau 2017]. In Sections 5 and 6, we proof Theorem 1.2 using the combinatorial identity of Heath-Brown's type, first by treating the case of rational parameters, and then by interpolating the obtained results to all functions in $\mathcal{F}_D(A)$. In Section 7, we sketch an alternative proof using the combinatorial identity of Linnik's type. Finally, in Section 8, we estimate the main terms and prove Theorems 1.3, 1.4 and 1.6.

2. First reductions

2A. *Statement of the main proposition.* For $n, h \in \mathbb{Z}$ with $n \geq 1$ and $n - h \geq 1$, let

$$\tilde{\tau}_h(n; R) := 2 \sum_{\substack{q \leq \sqrt{n-h} \\ (n,q)=(h,q)}} \frac{1}{\varphi\bigl(\frac{q}{(h,q)}\bigr)} \sum_{\substack{\chi \ (\mathrm{mod}\ q/(h,q)) \\ \mathrm{cond}(\chi) \leq R}} \chi\Bigl(\tfrac{h}{(h,q)}\Bigr)\overline{\chi\Bigl(\tfrac{n}{(h,q)}\Bigr)}. \tag{2-1}$$

Note that $\tilde{\tau}_h(n; R) = \tau(n-h)$ if $R > \sqrt{n-h}$ and $n-h$ is not a perfect square. We will eventually choose R of size $(\log n)^{O(1)}$. We have a trivial bound

$$\tilde{\tau}_h(n; R) \ll_\varepsilon n^\varepsilon R^{1+\varepsilon}. \tag{2-2}$$

The function $\tilde{\tau}_h(n; R)$ should be thought of as an approximation to $\tau(n-h)$ on average. The main work in proving Theorem 1.2 consists in showing that, for any $f \in \mathcal{F}_D(A)$, we have

$$\sum_{n \leq x} f(n)\tau(an-h) \sim \sum_{n \leq x} f(n)\tilde{\tau}_h(an; R_x) \quad \text{for } x \to \infty, \tag{2-3}$$

where R_x is some slowly growing function in x (some appropriate power of $\log x$). Once this is established, we can evaluate the sum on the right by standard methods. In view of this, it is convenient to define

$$\Delta_h(n; R) := \tau(n-h) - \tilde{\tau}_h(n; R) \quad \text{and} \quad \Sigma_f(I; a, h; R) := \sum_{n \in I} f(n)\Delta_h(an; R),$$

for any interval $I \subseteq \mathbb{R}^+$. The main part of this article is concerned with proving the following proposition, which puts the statement (2-3) into precise terms, and from which the results described in the introduction can be deduced easily (see Section 8).

Proposition 2.1. *Let $A, D \geq 1$ be fixed. Then we have, for $x \geq 3$, $I \subset [x/2, x]$ an interval and $f \in \mathcal{F}_D(A)$, the following estimate,*

$$|\Sigma_f(I; a, h; R)| \leq C\tau((a,h))\frac{x(\log x)^B}{R^{1/3}} \quad \textit{for } 1 \leq a, |h|, R \leq x^\delta, \tag{2-4}$$

where $\delta > 0$ is some absolute constant and where $B, C > 0$ are constants which depend only on A and D.

2B. *Restricting the set of functions.* It is known in multiplicative number theory that, to a certain degree of precision, the magnitude of the mean value of a multiplicative function f depends mostly on the values $f(p)$, p prime. The following lemma quantifies the analogous phenomenon in our case.

Lemma 2.2. *Let $f, g : \mathbb{N} \to \mathbb{C}$ be multiplicative functions, which satisfy the following conditions:*

(i) $|g(n)| \leq \tau_M(n)$ *for some $M \geq 1$ and all $n \in \mathbb{N}$.*

(ii) $H := \sum_{n \geq 1} |(f * g^{-1})(n)|/n^\sigma < +\infty$ *for some $\sigma < 1$, where g^{-1} denotes the Dirichlet convolution inverse of g.*

Furthermore, assume there are constants $\varrho, \delta \in (0, 1]$ *and* $B, C \geq 1$ *such that, for all* $x \geq 1$ *and all intervals* $I \subset [x/2, x]$,

$$|\Sigma_g(I; a, h; R)| \leq C\tau((a, h))\frac{x(\log x)^B}{R^{\varrho}} \quad \text{for } 1 \leq a, |h|, R \leq x^{\delta}. \tag{2-5}$$

Then there exists $C', \delta' > 0$ *depending only on* ϱ, δ, σ *and* M, *such that, for all* $x \geq 1$ *and all intervals* $I \subset [x/2, x]$,

$$|\Sigma_f(I; a, h; R)| \leq HCC'\tau((a, h))\frac{x(\log x)^B}{R^{\varrho}} \quad \text{for} \quad 1 \leq a, |h|, R \leq x^{\delta'}. \tag{2-6}$$

Proof. Let $h := f * g^{-1}$. We have

$$\begin{aligned}\Sigma_f(I; a, h; R) &= \sum_{n_1 n_2 \in I} g(n_1)h(n_2)\Delta_h(an_1n_2; R) \\ &= \sum_{n_2 \leq T} h(n_2)\Sigma_g(I/n_2; an_2, h; R) + \sum_{n_2 > T} h(n_2)\Sigma_g(I/n_2; an_2, h; R),\end{aligned}$$

for some parameter $T \geq 1$. For the sum on the left we use the assumption (2-5), so that

$$\sum_{n_2 \leq T} h(n_2)\Sigma_g(I/n_2; an_2, h; R) \ll_{\sigma} CH\tau((a, h))\frac{x(\log x)^B}{R^{\varrho}},$$

provided that the parameters a, h and R satisfy

$$1 \leq a \leq \frac{x^{\delta}}{T^{1+\delta}} \quad \text{and} \quad 1 \leq |h|, R \leq \frac{x^{\delta}}{T^{\delta}}.$$

For the sum on the right we use the trivial bound $\Sigma_g(I/n_2; an_2, h; R) \ll_{\varepsilon,M} Rx^{1+\varepsilon}/n_2$, and get

$$\sum_{n_2 > T} h(n_2)\Sigma_g(I/n_2; an_2, h; R) \ll_{\varepsilon,M} x^{1+\varepsilon}RT^{-1+\sigma}H.$$

The lemma follows on setting $T = x^{\delta/3}$ and $\delta' = \min(\delta/3, \delta(1-\sigma)/(4(1+\rho)))$. □

In view of this, in order to prove Proposition 2.1, we will restrict to the following two subsets of $\mathcal{F}_D(A)$. The first subset, denoted by $\mathcal{F}_D^{\tau}(A)$, consists of functions $f : \mathbb{N} \to \mathbb{C}$, which are the coefficients of Dirichlet series of the form

$$\sum_{n=1}^{\infty} \frac{f(n)}{n^s} = \prod_{\chi \bmod D} L(s, \chi)^{b_\chi}, \tag{2-7}$$

where the parameters b_χ are complex numbers such that $|b_\chi| \leq A$. Note that $\tau_z \in \mathcal{F}_D^{\tau}(A)$ for $|z| \leq A$. A particularly important role will be played by the subset $\mathcal{F}_D^{\tau_{\mathbb{Q}}}(A) \subset \mathcal{F}_D^{\tau}(A)$ formed by functions of this form where all the parameters b_χ are rational.

The second subset $\mathcal{F}_D^{\omega}(A)$ is defined to be the set of functions $f:\mathbb{N}\to\mathbb{C}$, which are the coefficients of Dirichlet series of the form

$$\sum_{n=1}^{\infty}\frac{f(n)}{n^s}=\prod_{r\in(\mathbb{Z}/D\mathbb{Z})^\times}\prod_{p\equiv r \bmod D}\Big(1+\frac{z_r}{p^s-1}\Big), \tag{2-8}$$

where the coefficients z_r are complex numbers such that $|z_r|\le A$. This includes the functions $n\mapsto z^{\omega(n)}$ for all $|z|\le A$.

Lemma 2.3. *For any $f\in\mathcal{F}_D(A)$, there exist $g_1\in\mathcal{F}_D^{\tau}(A)$ and $g_2\in\mathcal{F}_D^{\omega}(A)$ which satisfy the conditions (i)–(ii) stated in Lemma 2.2 for $\sigma=\frac{2}{3}$, and M, H bounded only in terms of A and D.*

Proof. We first prove the lemma with respect to the set $\mathcal{F}_D^{\tau}(A)$. Let $f\in\mathcal{F}_D(A)$ be fixed, and let $v_f:\mathbb{Z}\to\mathbb{C}$ be the D-periodic function defined by

$$v_f(r)=\begin{cases} f(p) & \text{if there exists a prime } p \text{ such that } (p,D)=1 \text{ and } p\equiv r \bmod D,\\ 0 & \text{if } (r,D)>1.\end{cases} \tag{2-9}$$

We then set

$$b_\chi:=\frac{1}{\varphi(D)}\sum_{r \pmod D} v_f(r)\overline{\chi}(r)\quad\text{for any character } \chi \bmod D,$$

and define g_1 as the coefficients of the following Dirichlet series,

$$\sum_{n=1}^{\infty}\frac{g_1(n)}{n^s}:=\prod_{\chi \pmod D} L(s,\chi)^{b_\chi}. \tag{2-10}$$

We have $(f*g_1^{-1})(p)=0$ if $p\nmid D$. Moreover, since $|b_\chi|\le A$, we get $|g_1(n)|\le\tau_{AD}(n)$ for all n. Therefore,

$$\sum_{n\ge1}\frac{|(f*g_1^{-1})(n)|}{n^{2/3}}=\prod_{p\mid D}\Big(1+\mathcal{O}_{A,D}\Big(\frac{1}{p^{2/3}}\Big)\Big)\prod_{p\nmid D}\Big(1+\mathcal{O}_{A,D}\Big(\frac{1}{p^{4/3}}\Big)\Big)=\mathcal{O}_{A,D}(1).$$

This proves the first part of the lemma.

For the second part, we define g_2 by its Dirichlet series

$$\sum_{n=1}^{\infty}\frac{g_2(n)}{n^s}:=\prod_{r\in(\mathbb{Z}/D\mathbb{Z})^\times}\prod_{\substack{p \text{ prime}\\ p\equiv r \bmod D}}\Big(1+\frac{v_f(r)}{p^s-1}\Big).$$

The fact that g_2 satisfies the required conditions can be shown using similar computations as above. □

Let us at this point also note the following result, which is an easy consequence of the proofs of Lemmas 2.2 and 2.3, and which will become useful later on.

Lemma 2.4. *Let $f \in \mathcal{F}_D(A)$ and let ψ mod q be a Dirichlet character. Then the Dirichlet series associated to ψf is given by*

$$\sum_{n=1}^{\infty} \frac{\psi(n) f(n)}{n^s} = H_\psi(s) \prod_{\chi \bmod D} L(s, \psi\chi)^{b_\chi} \quad \textit{for} \quad \mathfrak{Re}(s) > 1,$$

where $H_\psi(s)$ is some holomorphic function defined in $\mathfrak{Re}(s) > \frac{1}{2}$ and where

$$b_\chi := \frac{1}{\varphi(D)} \sum_{r \bmod D} v_f(r) \overline{\chi}(r),$$

with $v_f(n)$ as defined in (2-9). Moreover, for any fixed $\sigma_0 > \frac{1}{2}$, we have $H_\psi(s) \ll 1$ uniformly in $\mathfrak{Re}(s) > \sigma_0$, with the implicit constant depending at most on σ_0, A and D.

From Lemmas 2.2 and 2.3, we deduce the following statement.

Lemma 2.5. *To prove Proposition 2.1 in full generality, it suffices to prove it under either one of the additional hypotheses $f \in \mathcal{F}_D^\tau(A)$ or $f \in \mathcal{F}_D^\omega(A)$.*

3. Combinatorial identities for $\tau_z(n)$

In this section we describe the two combinatorial identities for the generalized divisor function τ_z on which the proofs of Theorem 1.2 are based.

3A. ***A generalization of Heath-Brown's identity.*** We first derive a combinatorial decomposition analogous to [Heath-Brown 1982] for the function $n \mapsto \tau_\alpha(n)$ in the case $\alpha \in \mathbb{Q}$. Our argument is based on the following polynomial identity.

Lemma 3.1. *Let u and v be integers such that $v > u \geq 0$. Let $K \geq 1$ and $N \geq 0$. Then there exist rational coefficients a_m and b_ℓ such that there holds*

$$\sum_{K \leq m \leq (K+N)v-u} a_m (X-1)^m = 1 + X^{Nv} \sum_{1 \leq \ell \leq K} b_\ell X^{\ell v - u}. \tag{3-1}$$

The coefficients (b_ℓ) are unique and given explicitly by

$$b_\ell = \frac{(-1)^\ell}{(\ell-1)!(K-\ell)!} \prod_{\substack{1 \leq j \leq K \\ j \neq \ell}} \left(j + N - \frac{u}{v}\right). \tag{3-2}$$

Proof. An identity of the form (3-1) exists if and only if we can find $b_1, \dots, b_K$ such that the first $K-1$ derivatives of the polynomial on the right hand side of (3-1) vanish at $X = 1$. This is equivalent to saying that the $b_1, \dots, b_K$ solve the equation

$$\begin{pmatrix} 1 & \cdots & 1 \\ v+Nv-u & \cdots & Kv+Nv-u \\ \vdots & \ddots & \vdots \\ (v+Nv-u)^{K-1} & \cdots & (Kv+Nv-u)^{K-1} \end{pmatrix} \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_K \end{pmatrix} = \begin{pmatrix} -1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}. \tag{3-3}$$

Let C be the matrix on the left, and B_ℓ the same matrix but with the upper row and the ℓ-th column removed. Note that C is a Vandermonde matrix, and B_ℓ is a product of a Vandermonde matrix with a diagonal matrix. Hence, we deduce

$$\det C = \prod_{1\le i<j\le K} (jv-iv) = 2!3!\cdots(K-1)!v^{K(K-1)/2},$$

$$\det B_\ell = \prod_{\substack{1\le i<j\le K\\ i,j\ne\ell}} (jv-iv) \prod_{\substack{1\le j\le K\\ j\ne\ell}} (jv+Nv-u).$$

Since $\det C \ne 0$, we obtain by Cramer's rule that there is a unique solution (b_ℓ), given by

$$b_\ell = (-1)^\ell \frac{\det B_\ell}{\det C}, \tag{3-4}$$

which yields (3-2). □

Theorem 3.2. *Let $v > 0$ and r be integers such that $v > u \ge 0$ and $r \ge 0$. Let $K \ge 1$ and $x \ge 1$. Then for any $n \le x$, we have*

$$\tau_{r+u/v}(n) = \sum_{\ell=1}^{K} c_\ell^+ \sum_{\substack{m_1\cdots m_{\ell+r} n_1\cdots n_{\ell v-u}=n\\ n_1,\dots,n_{\ell v-u}\le x^{1/K}}}\!\!\cdots\sum \tau_{-1/v}(n_1)\cdots\tau_{-1/v}(n_{\ell v-u}), \tag{3-5}$$

and, for $r \ge 1$,

$$\tau_{-r+u/v}(n) = \sum_{\ell=1}^{K} c_\ell^- \sum_{\substack{m_1\cdots m_{\ell-1} n_1\cdots n_{\ell v+(r-1)v-u}=n\\ n_1,\dots,n_{\ell v+(r-1)v-u}\le x^{1/K}}}\!\!\cdots\sum \tau_{-1/v}(n_1)\cdots\tau_{-1/v}(n_{\ell v+(r-1)v-u}), \tag{3-6}$$

where the c_ℓ^+ and c_ℓ^- are certain rational numbers, which can be bounded by

$$c_\ell^+, c_\ell^- \ll 1 \quad \text{for } 1 \le \ell \le K,$$

the implicit constant depending only on K and r.

Proof. Let

$$G(s) := \sum_{n=1}^{\infty} \frac{\tau_{-1/v}(n)g(n)}{n^s} \quad \text{with} \quad g(n) := \begin{cases} 1 & \text{if } n \le x^{1/K}, \\ 0 & \text{otherwise.} \end{cases}$$

We first look at (3-5). Here we use Lemma 3.1 with $N=0$ and $X=\zeta(s)^{\frac{1}{v}}G(s)$, and then multiply both sides by $\zeta(s)^{r+u/v}$, which leads to the identity

$$\sum_{K\le m\le Kv-u} a_m(\zeta(s)^{1/v}G(s)-1)^m\zeta(s)^{r+u/v}=\zeta(s)^{r+u/v}+\sum_{1\le\ell\le K} b_\ell\zeta(s)^{r+\ell}G(s)^{\ell v-u}.$$

Then (3-5) follows by comparing the Dirichlet coefficients on both sides and noting that, by construction, the left-hand side has no Dirichlet coefficient for $n\le x$.

In order to show (3-6), we use Lemma 3.1 with the same X as before and with $N=r-1$, and then multiply both sides by $\zeta(s)^{-r+\frac{u}{v}}$. This gives

$$\sum_{K\le m\le(K+r-1)v-u} a_m\Big(\zeta(s)^{1/v}G(s)-1\Big)^m\zeta(s)^{-r+u/v}=\zeta(s)^{-r+u/v}+\sum_{1\le\ell\le K} b_\ell\zeta(s)^{\ell-1}G(s)^{\ell v+(r-1)v-u},$$

and (3-6) follows again by comparing the Dirichlet coefficients on both sides. □

Remark. With $r=v=1$ and $u=0$, the identity (3-6) leads to the decomposition of $\mu(n)$ described in [Iwaniec and Kowalski 2004, (13.38)].

3B. ***A combinatorial identity of Linnik's type.*** Here we derive a combinatorial decomposition for τ_z using an approach analogous to [Linnik 1963].

We denote by $P^+(n)$ the largest, and by $P^-(n)$ the smallest prime factor of an integer $n>1$, with the convention that $P^+(1)=1$ and $P^-(1)=\infty$. Given an arbitrary multiplicative function f and a complex number $z\in\mathbb{C}$, we define the z-fold convolution of f as the multiplicative function given by

$$f^{(*z)}(p^\nu):=\sum_{1\le r\le\nu}\binom{z}{r}\sum_{\substack{\lambda_1,\dots,\lambda_r\ge1\\ \lambda_1+\dots+\lambda_r=\nu}} f(p^{\lambda_1})\cdots f(p^{\lambda_r})(\nu\ge1).$$

The notation is motivated by the fact that if $F(s):=\sum_{n\ge1}f(n)n^{-s}$ is the Dirichlet series associated to f, then for $\mathfrak{Re}(s)$ large enough the function $\log F(s)$ is well defined and we have $F(s)^z=\sum_n f^{(*z)}(n)n^{-s}$. Indeed, by expressing $F(s)$ as an Euler product, we see immediately that

$$F(s)^z=\prod_p\Big(1+\sum_{\nu\ge1}\frac{f(p^\nu)}{p^{\nu s}}\Big)^z=\prod_p\Big(1+\sum_{r\ge1}\binom{z}{r}\Big(\sum_{\nu\ge1}\frac{f(p^\nu)}{p^{\nu s}}\Big)^r\Big)=\prod_p\Big(1+\sum_{\nu\ge1}\frac{f^{(*z)}(p^\nu)}{p^{\nu s}}\Big).$$

Note that $f^{(*z)}(p)=zf(p)$, and that for $\ell\in\mathbb{N}$ the ℓ-fold convolution as defined here coincides with the ℓ-fold convolution defined in the traditional sense. We will be eventually interested in the case when $f=\chi$ is a Dirichlet character, in which case we have $f^{(*z)}=\tau_z^\chi$.

Theorem 3.3. *Let $K\in\mathbb{N}_{>0}$ and $A,x\ge1$. Then for all $z\in\mathbb{C}$ there exist complex numbers $(c_\ell)_{0\le\ell\le K}$, such that for all $x\ge1$ and all multiplicative functions f, we have the following identity for $n\le x$,*

$$f^{(*z)}(n)=\sum_{0\le\ell<K}c_\ell\sum_{\substack{n=n_1n_2\\ P^+(n_1)\le x^{1/K}}} f^{(*(z-\ell))}(n_1)f^{(*\ell)}(n_2), \tag{3-7}$$

where the coefficients c_ℓ can be bound by $c_\ell=O_{K,A}(1)$ uniformly for $|z|\le A$.

Proof. Let $y := x^{1/K}$. As before we set $F(s) := \sum_{n\geq 1} f(n)n^{-s}$. We may certainly assume that $f(p^k)$ vanishes if $p > x$. Let

$$F(s, y) = \prod_{p\leq y}\Big(\sum_{k\geq 0} \frac{f(p^k)}{p^{ks}}\Big), \quad G(s, y) = \prod_{p>y}\Big(\sum_{k\geq 0} \frac{f(p^k)}{p^{ks}}\Big).$$

For $\mathfrak{Re}(s) > 0$, the decomposition $F(s) = F(s, y)G(s, y)$ yields

$$\begin{aligned} F(s)^z &= F(s, y)^z(1 + (G(s, y) - 1))^z \\ &= F(s, y)^z \sum_{k\geq 0} \binom{z}{k}(G(s, y) - 1)^k \\ &= F(s, y)^z \sum_{0\leq k<K} \binom{z}{k}(G(s, y) - 1)^k + R(s) \end{aligned}$$

with

$$R(s) := F(s, y)^z \sum_{k\geq K} \binom{z}{k}(G(s, y) - 1)^k.$$

Note that the series converge absolutely if $\mathfrak{Re}(s)$ is large enough in terms of f. By expanding, we get

$$F(s)^z = F(s, y)^z \sum_{0\leq \ell<K} c_\ell G(s, y)^\ell + R(s),$$

with

$$c_\ell := (-1)^\ell \sum_{\ell\leq k<K} (-1)^k \binom{z}{k}\binom{k}{\ell}.$$

We read the coefficients of n^{-s}, for $n \leq x$, on each side. Note that for $k \geq K$, the series $(G(s, y) - 1)^k$ has no corresponding Dirichlet coefficients, so there is no contribution from $R(s)$. The claimed equality follows on writing $G(s, x^{1/K}) = F(s)F(s, x^{1/K})^{-1}$. □

Remarks. • Compared with (3-5)–(3-6), this identity has the significant advantage that it is uniform for $z \ll 1$ complex.

• The case $K = 2$ only involves the exponents $\ell \in \{0, 1\}$. It follows, for instance, that if $f^{(*z)}$ satisfies a Siegel–Walfisz estimate (in the sense of [Granville and Shao 2018, equation (1.2)]), and if f satisfies a Bombieri–Vinogradov theorem, then $f^{(*z)}$ satisfies a Bombieri–Vinogradov theorem as well.

• The case $K = 2$, $f = \mathbf{1}$ leads to Eratosthenes' sieve identity: for all $n \in (\sqrt{x}, x]$, we have

$$\mathbf{1}_{n \text{ prime}} = \sum_{\substack{d\,|\,n \\ p\,|\,d \Rightarrow p\leq\sqrt{x}}} \mu(d).$$

For any $\eta \in (0, 1/2)$, either we have $d \leq x^\eta$ (which corresponds to type I sums), or $d > x^\eta$, in which case we can localize a factor of d in the interval $[x^\eta, x^{1/2+\eta}]$ (and this corresponds to type II sums).

The main property which allows Theorem 3.3 to be used in our arguments is the following factorization lemma, in the spirit of Lemma 3.1 of [Vaughan 1989, page 29]; see [Hmyrova 1964] for an early use of this property, and [Fouvry and Tenenbaum 1996] for an application in a context similar to ours.

Lemma 3.4. *For any multiplicative function $f:\mathbb{N}\to\mathbb{R}$, any compactly supported function $g:\mathbb{N}\to\mathbb{C}$, and all $y, w\geq 2$, we have*

$$\sum_{P^+(n)\leq y} f(n)g(n) = \Sigma_{\mathrm{triv}} + \Sigma_I + \mathcal{O}(\Sigma_{\mathrm{II}}), \tag{3-8}$$

where

$$\Sigma_{\mathrm{I}} = \sum_{\substack{n\leq w\\ P^+(n)\leq y}} f(n)g(n), \quad \Sigma_{\mathrm{triv}} = \sum_{\substack{n>w\\ P^+(n)\leq y\\ \exists p^\nu \,\|\, n,\, p^\nu>y}} f(n)g(n), \quad \Sigma_{\mathrm{II}} = (\log y)\sup_{\alpha,\beta}\Bigl|\sum_{w<m\leq yw}\sum_n \alpha_m\beta_n g(mn)\Bigr|,$$

the supremum in Σ_{II} being taken over all sequences (α_m), (β_n) of complex numbers satisfying

$$|\alpha_m|\leq |f(m)|, \quad |\beta_n|\leq (|f|*|f|)(n).$$

Proof. If an integer n with $P^+(n)\leq y$ is not counted in the first two sums on the right-hand side, then $n>w$ and all prime powers $p^\nu \,\|\, n$ satisfy $p^\nu\leq y$. By incorporating these prime powers as p increases, we may factor $n=n_1n_2$ uniquely in such a way that

$$P^+(n_1)<P^-(n_2), \quad w<n_1\leq wQ^+(n_1),$$

where $Q^+(n_1)$ is the prime power corresponding to the largest prime of n_1: $Q^+(n_1)=P^+(n_1)^\nu \,\|\, n_1$. Note that this implies $(n_1,n_2)=1$. Our statement follows after separating variables [Iwaniec and Kowalski 2004, Lemma 13.11] in the condition $P^+(n_1)<P^-(n_2)$. □

4. Auxiliary estimates

In this section we collect some estimates on $\Delta_h(n, R)$, which will be needed in the following sections.

4A. ***The second moment of $\Delta_h(n;R)$.*** On several occasions, we will require the following rough upper-bound for the "main terms".

Lemma 4.1. *For $x\geq 3$, $R\geq 1$ and $(a,h)\in\mathbb{Z}^2$ such that $1\leq a, |h|, R\leq x^{1/4}$, the following estimate holds,*

$$\sum_{x/2<n\leq x} |\Delta_h(an;R)|^2 \ll \tau((a,h))^2 x(\log x)^4.$$

Proof. We have

$$\sum_{x/2<n\leq x} |\Delta_h(an;R)|^2 \ll \sum_{x/2<n\leq x}\tau(an-h)^2 + \sum_{x/2<n\leq x}|\tilde{\tau}_h(an;R)|^2 =: G_1+G_2,$$

and we now proceed to estimate the two sums G_1 and G_2 separately.

We first look at G_1. For notational convenience, let

$$a' := \frac{a}{(a,h)}, \quad h' := \frac{h}{(a,h)} \quad \text{and} \quad t := (a,h).$$

We start by splitting the sum according to the size of $t^* = (an-h, t^\infty)$ as follows,

$$G_1 = \sum_{\substack{t^* \mid t^\infty \\ (t^*,a')=1 \\ t^* \le x^{1/2}}} \sum_{\substack{x/2<n\le x \\ a'n\equiv h' \bmod t^* \\ ((a'n-h')/t^*,t)=1}} \tau(an-h)^2 + \sum_{\substack{t^* \mid t^\infty \\ (t^*,a')=1 \\ t^* > x^{1/2}}} \sum_{\substack{x/2<n\le x \\ a'n\equiv h' \bmod t^* \\ ((a'n-h')/t^*,t)=1}} \tau(an-h)^2 =: G_{1\mathrm{a}} + G_{1\mathrm{b}}.$$

In order to estimate $G_{1\mathrm{a}}$ we choose $b, y \in \mathbb{Z}$ such that $a'b = 1 + yt^*$ and write

$$\begin{aligned} G_{1\mathrm{a}} &= \sum_{\substack{t^* \mid t^\infty \\ (t^*,a')=1 \\ t^* \le x^{1/2}}} \tau(t^* t)^2 \sum_{\substack{(x-2bh')/2t^* < n' \le (x-bh')/t^* \\ (yh'+n'a',t)=1}} \tau(yh'+n'a')^2 \\ &\le \sum_{\substack{t^* \mid t^\infty \\ (t^*,a')=1 \\ t^* \le x^{1/2}}} \tau(t^* t)^2 \sum_{\substack{(a'x-2h')/2t^* < m \le (a'x-h')/t^* \\ m\equiv yh' \bmod a'}} \tau(m)^2. \end{aligned}$$

The sum over m can now be estimated via [Shiu 1980, Theorem 2] or [Barban and Vehov 1969, Theorem 1], which leads to

$$G_{1\mathrm{a}} \ll x \log^3 x \sum_{\substack{t^* \mid t^\infty \\ t^* \le x^{1/2}}} \frac{\tau(t^* t)^2}{t^*} \ll \tau((a,h))^2 x \log^4 x. \tag{4-1}$$

In $G_{1\mathrm{b}}$ we bound all the summands trivially and get

$$G_{1\mathrm{b}} \ll \sum_{\substack{t^* \mid t^\infty \\ (t^*,a')=1 \\ t^* > x^{1/2}}} \sum_{\substack{x/2<n\le x \\ a'n\equiv h' \bmod t^*}} \tau(t(a'n-h'))^2 \ll x^{1+\varepsilon} \sum_{\substack{t^* \mid t^\infty \\ x^{1/2} < t^* \le 2a'x}} \frac{1}{t^*} \ll x^{3/4+\varepsilon},$$

so that together with (4-1) we deduce

$$G_1 \ll \tau((a,h))^2 x \log^4 x.$$

Next we look at G_2. Here we first rewrite $\tilde{\tau}_h(an; R)$ as

$$\tilde{\tau}_h(an; R) := 2 \sum_{\alpha \mid (a,h)} \sum_{\substack{\delta \mid (h/\alpha, n) \\ (\delta, a/\alpha)=1}} \sum_{q \le \sqrt{an-h}/(\alpha\delta)} \frac{1}{\varphi(q)} \sum_{\substack{\chi \pmod q \\ \mathrm{cond}(\chi) \le R}} \chi\big(\tfrac{h}{\alpha\delta}\big) \overline{\chi\big(\tfrac{an}{\alpha\delta}\big)},$$

so that after expanding the square we are led to

$$G_2 \le 4 \sum_{\substack{\alpha_1,\alpha_2 \mid (a,h) \\ \delta_1 \mid h/\alpha_1, \delta_2 \mid h/\alpha_2}} \sum_{\substack{q_1 \le \sqrt{ax-h}/(\alpha_1\delta_1) \\ q_2 \le \sqrt{ax-h}/(\alpha_2\delta_2)}} \frac{1}{\varphi(q_1)\varphi(q_2)} \sum_{\substack{\chi_1 \pmod{q_1} \\ \chi_2 \pmod{q_2} \\ \mathrm{cond}(\chi_1),\mathrm{cond}(\chi_2) \le R}} S\big(\overline{\chi}_1 \chi_2, \tfrac{x}{[\delta_1,\delta_2]}\big),$$

with

$$S(\chi, y) := \max_{y/2 \le y_0 < y} \Big| \sum_{y_0 < n \le y} \chi(n) \Big|.$$

If χ_1 and χ_2 are induced by the same primitive character, we use the trivial bound $S(\bar{\chi}_1\chi_2, y) \le y$. Otherwise, the Pólya–Vinogradov bound applies and $S(\bar{\chi}_1\chi_2, y) \ll \tau(q_1q_2)R\log R$. Inserting these bounds, we eventually obtain

$$G_2 \ll \tau((a,h))^2 x \log^4 x + x^\varepsilon R^3 \ll \tau((a,h))^2 x \log^4 x$$

by our assumption $R \le x^{1/4}$. This concludes the proof. □

4B. *Comparison of main terms.* We begin by two technical lemmas related to the main terms that will appear later. Let $X \ge 1$, and let f and v be two smooth functions which are both compactly supported inside $\mathbb{R}_+^*$. We assume that $\operatorname{supp} f \subset [C_1X, C_2X]$ and $\operatorname{supp} v \subset [C_1, C_2]$, where C_1 and C_2 are some positive constants, and that for some $\Omega \in (0, 1]$, we have

$$\|v^{(j)}\|_\infty \ll_j 1, \quad \|f^{(j)}\|_\infty \ll_j (\Omega X)^{-j}, \quad \int_{\mathbb{R}} |f^{(j+1)}| \ll (\Omega X)^{-j}, \tag{4-2}$$

for all $j \ge 0$. Furthermore, we define

$$M_{f,v}(b,h;M) := \frac{1}{b}\sum_{d\,|\,b} \frac{c_d(h)}{d} \int (\log(\xi - h) + 2\gamma - 2\log d) f(\xi) v\Big(\frac{\xi}{bM}\Big)\, d\xi, \tag{4-3}$$

where

$$c_d(h) := \sum_{\nu (\mathrm{mod}^* d)} \mathrm{e}(\nu h/d) = \sum_{\delta\,|\,(h,d)} \delta\mu(d/\delta)$$

denotes the Ramanujan sum.

Lemma 4.2. *For $(b,h) \in \mathbb{Z}^2$, $b, M \ge 1$, and $R \ge 1$, we have*

$$\sum_m f(bm) v\Big(\frac{m}{M}\Big) \tilde{\tau}_h(bm; R) = M_{f,v}(b,h;M) + \mathcal{O}\Big(X^\varepsilon R^{3/2} + X^{1/2+\varepsilon}\frac{(h,b)}{b}\Big),$$

where the implied constant depends on ε, C_1, C_2 and on the implied constants in (4-2).

Proof. By partial summation and the Pólya–Vinogradov inequality, given a character $\chi \pmod{q/(q,h)}$ of conductor $1 < r \le R$, we have

$$\sum_n f(bm) v\Big(\frac{m}{M}\Big) \chi\Big(\frac{bm}{(h,q)}\Big) = \chi\Big(\frac{b}{(b,q)}\Big) \iint f'(t_1) v'(t_2) \sum_{\substack{m \ge \frac{h+q^2}{(h,q)/(b,q)} \\ m \le \frac{t_1/b + Mt_2}{(h,q)/(b,q)}}} \chi(m)\mathrm{d}t_1\mathrm{d}t_2 \ll R^{1/2} q^\varepsilon.$$

By definition (2-1), we deduce

$$\sum_m f(bm) v\Big(\frac{m}{M}\Big) \tilde{\tau}_h(bm; R) = 2\sum_m f(bm) v\Big(\frac{m}{M}\Big) \sum_{\substack{q \le \sqrt{bm-h} \\ (bm,q)=(h,q)}} \frac{1}{\varphi(q/(q,h))} + \mathcal{O}(X^\varepsilon R^{3/2}).$$

The condition $(bm, q) = (h, q)$ in the sum on the right-hand side is equivalent to

$$(b, q) \mid h, \quad \frac{(h, q)}{(b, q)} \Big| m, \quad \left(\frac{m(b, q)}{(h, q)}, \frac{q}{(h, q)} \right) = 1.$$

Using Möbius inversion and our hypotheses on f and v, we can replace the m-sum by the corresponding integral and obtain

$$\sum_m f(bm) v\left(\frac{m}{M}\right) \tilde{\tau}_h(bm; R) = \frac{2}{b} \int f(\xi) v\left(\frac{\xi}{bM}\right) \sum_{\substack{q \le \sqrt{\xi - h} \\ (b,q) \mid h}} \frac{(b, q)}{q} \, \mathrm{d}\xi + \mathcal{O}(X^\varepsilon R^{3/2}).$$

The main term on the right-hand side may be rewritten as

$$\frac{2}{b} \sum_{d \mid b} \frac{c_d(h)}{d} \int f(\xi) v\left(\frac{\xi}{bM}\right) H\left(\frac{\sqrt{\xi - h}}{d}\right) \mathrm{d}\xi + \mathcal{O}(X^\varepsilon R^{3/2})$$

where $H(x) = \sum_{q \le x} 1/q = \log x + \gamma + \mathcal{O}(x^{-1})$. This gives the claimed estimate. □

Next, we define

$$M^{\chi}_{f,v}(b, h; M) := \sum_{\substack{a \bmod D \\ (a,D)=1}} \chi(a) M_{f_{ab}, v_{a/M}}(bD, h - ab; M/D) \tag{4-4}$$

where $f_{ab}(\xi) := f(\xi + ab)$ and $v_{a/M}(\xi) := v(\xi + a/M)$.

Lemma 4.3. *If* $b = b^\circ b^*$ *with* $b^\circ \mid D^\infty$ *and* $(b^*, D) = 1$, *then*

$$M^{\chi}_{f,v}(b, h; M) = \frac{1}{bD} \chi\left(\frac{h}{(h, b)}\right) \bar{\chi}\left(\frac{b}{(h, b)}\right) \sum_{d \mid b^*} \frac{c_d(h)}{d} \int \left(\log\left(\frac{\xi - h}{(Db^\circ d)^2}\right) + 2\gamma \right) f(\xi) v\left(\frac{\xi}{bM}\right) \mathrm{d}\xi. \tag{4-5}$$

Moreover, if $\chi \bmod D$ *is primitive, we have*

$$\sum_m f(bm) v\left(\frac{m}{M}\right) \chi(m) \tilde{\tau}_h(bm; R)$$
$$= M^{\chi}_{f,v}(b, h; M) + \mathcal{O}\left(\mathbf{1}_{D>R}(b, h) \frac{X(\log X)^3}{bD} + X^\varepsilon D^{1/2} R^{3/2} + X^{1/2+\varepsilon} \frac{(h, b^*)}{b^*} \right)$$

where $\mathbf{1}_{D>R} = 1$ *if* $D > R$ *and* 0 *otherwise.*

Proof. We rewrite

$$M^{\chi}_{f,v}(b, h; M) = \frac{1}{bD} \sum_{\substack{a \ (\mathrm{mod}\ D) \\ (a,D)=1}} \chi(a) \sum_{d \mid bD} \frac{c_d(h - ab)}{d} \int (\log(\xi - h) + 2\gamma - 2\log d) f(\xi) v\left(\frac{\xi}{bM}\right) \mathrm{d}\xi.$$

Using Gauss sums,

$$\sum_{\substack{a \pmod D\\(a,D)=1}} \chi(a)c_d(h-ab) = G(\chi)\bar\chi\Big(\frac{-bD}{d}\Big) \sum_{\nu \pmod{^*d}} \bar\chi(\nu)\mathrm{e}\Big(\frac{h\nu}{d}\Big).$$

This last expression vanishes unless $D(b, D^\infty) \mid d$. Denoting $b^\circ = (b, D^\infty)$ and $b^* = b/b^\circ$, we obtain for $d \mid b^*$

$$\begin{aligned}\sum_{\substack{a \pmod D\\(a,D)=1}} \chi(a)c_{Db^\circ d}(h-ab) &= G(\chi)\bar\chi(-b^*/d)G(\bar\chi) \sum_{\delta \mid (b^\circ d,h)} \delta\chi(h/\delta)\mu(b^\circ d/\delta)\bar\chi(b^\circ d/\delta)\\ &= b^\circ D \mathbf{1}_{b^\circ \mid h}\bar\chi(b^*)\chi(h/b^\circ)c_d(h)\\ &= b^\circ D\chi\Big(\frac{h}{(h,b)}\Big)\bar\chi\Big(\frac{b}{(h,b)}\Big)c_d(h).\end{aligned}$$

This yields our first claim.

For the second, the computations are similar to the previous lemma. If $D > R$, we get

$$\sum_m f(bm)v\Big(\frac{m}{M}\Big)\chi(m)\tilde\tau_h(bm;R) \ll X^\varepsilon D^{1/2}R^{3/2}, \tag{4-6}$$

while on the other hand $M^{\chi}_{f,v}(b,h;M) \ll (b,h)(bD)^{-1}X(\log X)^2$ by a simple computation from (4-5). If $D \le R$, the bound (4-6) applies to all the characters involved in the definition of $\tilde\tau_h(bm;R)$, except all those which are induced by χ. We obtain

$$\begin{aligned}&\sum_m f(bm)v\Big(\frac{m}{M}\Big)\chi(m)\tilde\tau_h(bm;R)\\ &\qquad = 2\sum_{D \mid q/(q,h)} \frac{\chi(h/(b,q))\bar\chi(b/(b,q))}{\varphi(q/(h,q))} \sum_{\substack{(bm,q)=(h,q)\\ q^2\le bm-h}} f(bm)v\Big(\frac{m}{M}\Big) + \mathcal{O}(X^\varepsilon D^{1/2}R^{3/2}).\end{aligned}$$

Similarly as above, the main term in the right-hand side can be rewritten

$$\frac{2}{b}\chi\Big(\frac{h}{(h,b)}\Big)\bar\chi\Big(\frac{b}{(h,b)}\Big)\int f(\xi)v\Big(\frac{\xi}{bM}\Big) \sum_{\substack{q\le\sqrt{\xi-h}\\ (b,q)\mid h,\ D\mid q/(h,q)\\ (D,(b,h)/(b,q))=1}} \frac{(q,b)}{q}\,\mathrm{d}\xi + \mathcal{O}(X^\varepsilon)$$

The χ-factors impose the conditions $b^\circ \mid h$ and $(D, h/b^\circ) = 1$. We rewrite the q-sum as

$$\sum_{\substack{q\le\sqrt{\xi-h}\\ (b,q)\mid h,\ D\mid q/(h,q)\\ (D,(b,h)/(b,q))=1}} \frac{(b,q)}{q} = \frac{1}{D}\sum_{\substack{q\le\sqrt{\xi-h}/(Db^\circ)\\ (b^*,q)\mid h}} \frac{(q,b^*)}{q} = \frac{1}{D}\sum_{d\mid b^*}\frac{c_d(h)}{d}H\Big(\frac{\sqrt{\xi-h}}{Db^\circ d}\Big)$$

whence the claimed expression. □

4C. *Type τ_1 estimates.* The following estimate is relevant for convolutions with one smooth component of size $\gg x^{1/3+\varepsilon}$. It can be viewed as a generalization of a result of Selberg [1991, page 235] on the equidistribution of τ_2 in arithmetic progressions.

Lemma 4.4. *Let $\varepsilon > 0$, let $C_2 > C_1 > 0$, let $v : (0,\infty) \to \mathbb{R}$ be a smooth and compactly supported function, and let $\chi \bmod D$ be a Dirichlet character of modulus $D \geq 1$. Then we have, for any $X, M \geq 1$ and $R \geq D$, any $1 \leq bD$, $|h| \ll X^{1-\varepsilon}$, and any interval $I \subset [C_1X, C_2X]$,*

$$\sum_{m:bm\in I} \chi(m) v\Big(\frac{m}{M}\Big) \Delta_h(bm; R) \ll X^{\varepsilon}(DX^{1/3} + (b, hD^{\infty}) M X^{-1/2} + D^{1/2}R^3/2). \tag{4-7}$$

The implied constants depend only on the function v and the constants ε, C_1 and C_2.

Proof. Note that we can always assume $bM \asymp X$, since otherwise the sums in consideration are empty. Let $f : (0,\infty) \to [0,\infty)$ be a smooth weight function, which is compactly supported in $\operatorname{supp} f \subset [C_1X/2, 2C_2X]$, which has value $f(\xi) = 1$ for all $\xi \in I$, and whose derivatives satisfy

$$f^{(\nu)}(\xi) \ll \frac{1}{(\Omega X)^{\nu}} \quad \text{for } \nu \geq 0 \quad \text{and} \quad \int |f^{(\nu)}(\xi)|\, d\xi \ll \frac{1}{(\Omega X)^{\nu-1}} \quad \text{for } \nu \geq 1,$$

for some constant $\Omega \leq 1$. We can then encode the condition $bm \in I$ by using the function $f(\xi)$ via

$$\sum_{m:bm\in I} \chi(m) v\Big(\frac{m}{M}\Big) \Delta_h(bm; R) = \sum_{m} f(bm) v\Big(\frac{m}{M}\Big) \chi(m) \Delta_h(bm; R) + \mathcal{O}(\Omega X^{1+\varepsilon} b^{-1}), \tag{4-8}$$

so that it suffices to consider the smoothed sum on the right-hand side.

Assume first that χ is the trivial character. In [Topacogullari 2018, Section 3] it is shown that

$$\sum_{m} f(bm) v\Big(\frac{m}{M}\Big) \tau(bm - h) = M_{f,v}(b, h; M) + \mathcal{O}(X^{\varepsilon} b^{1/2} \Omega^{-1/2}), \tag{4-9}$$

where the main term $M_{f,v}(b, h; M)$ is given by (4-3). By Lemma 4.2, we obtain

$$\sum_{m} f(bm) v\Big(\frac{m}{M}\Big) \tilde{\tau}_h(bm; R) = M_{f,v}(b, h; M) + \mathcal{O}(X^{\varepsilon} R^{3/2} + (b, h) b^{-1} X^{1/2+\varepsilon}). \tag{4-10}$$

The estimate (4-7), in the case $D = 1$ and $\chi = \mathbf{1}$, now follows from (4-8) with the choice $\Omega = bX^{-2/3}$.

Now assume that χ is a primitive character modulo D, where $D \leq R$ and $bD \ll X^{1-\varepsilon}$. We write

$$\sum_{m} f(bm) v\Big(\frac{m}{M}\Big) \chi(m) \tau(bm - h) = \sum_{\substack{a \ (\mathrm{mod}\ D) \\ (a,D)=1}} \chi(a) \bigg(\sum_{m} \tilde{f}(\tilde{b}m) \tilde{v}\Big(\frac{m}{\tilde{M}}\Big) \tau(\tilde{b}m - \tilde{h}) \bigg),$$

with

$$\tilde{b} := Db, \quad \tilde{M} := M/D, \quad \tilde{h} := h - ab, \quad \tilde{f}(\xi) := f(\xi + ab) \quad \text{and} \quad \tilde{v}(\xi) := v\Big(\xi + \frac{a}{M}\Big),$$

so that we can use our former result (4-9) to get

$$\sum_m f(bm)v\left(\frac{m}{M}\right)\chi(m)\tau(bm-h) = M_{f,v}^{\chi}(b,h;M) + \mathcal{O}(X^{\varepsilon}D^{3/2}b^{1/2}\Omega^{-1/2}),$$

where $M_{f,v}^{\chi}(b,h;M)$ is defined in (4-4). By Lemma 4.3, we obtain

$$\sum_m f(bm)v\left(\frac{m}{M}\right)\chi(m)\tau(bm-h)$$
$$= \sum_m f(bm)v\left(\frac{m}{M}\right)\chi(m)\tilde{\tau}_h(bm;R) + O_{\varepsilon}\left(X^{\varepsilon}D^{3/2}b^{1/2}\Omega^{-1/2} + X^{\varepsilon}D^{1/2}R^{3/2} + X^{1/2+\varepsilon}\frac{(h,b^*)}{b^*}\right)$$

We choose $\Omega = bDX^{-2/3}$, and hence get (4-7) also in this case.

The case when χ is not necessarily primitive follows at once using Möbius inversion. □

4D. *Type τ_2 estimates.* The following estimate is a uniform version of the $\tau_2 - \tau_2$ shifted convolution problem obtained recently by the second author.

Lemma 4.5. *Let $\varepsilon > 0$, let $C_2 > C_1 > 0$, let $v_1, v_2 : (0,\infty) \to \mathbb{R}$ be smooth and compactly supported weight functions, and let χ_1 and χ_2 be Dirichlet characters mod D. Then for any $X, b \geq 1$ and $R \geq D$, any $M_1 \geq M_2 \geq 1$ with $X^{1/2} \leq M_1M_2$, any $h \in \mathbb{Z}$ with $1 \leq |h|$, $D \leq X^{1/4}$ and any interval $I \subset [C_1X/2, C_2X]$, we have*

$$\sum_{\substack{m_1,m_2:\\ bm_1m_2\in I}} v_1\left(\frac{m_1}{M_1}\right)v_2\left(\frac{m_2}{M_2}\right)\chi_1(m_1)\chi_2(m_2)\Delta_h(bm_1m_2;R)$$
$$\ll b^{\circ}D^{5/2}(XM_1M_2)^{1/3+\varepsilon}\left(1+\left(\frac{|h|M_1M_2}{XD}\right)^{1/4}\right) + X^{-1/2+\varepsilon}R^{3/2}b^{\circ}(h,b)M_1M_2^2. \tag{4-11}$$

The implied constant depends only on the constants ε, C_1 and C_2, and the functions v_1 and v_2.

Proof. Note that we can make the assumption $b \asymp \frac{X}{M_1M_2}$, as otherwise the sum in consideration is empty. Also, as in Lemma 4.4, we can exchange the original sum by its smoothed version,

$$\sum_{m_1,m_2} f(bm_1m_2)v_1\left(\frac{m_1}{M_1}\right)v_2\left(\frac{m_2}{M_2}\right)\chi_1(m_1)\chi_2(m_2)\Delta_h(bm_1m_2;R),$$

with an error of the size of $\mathcal{O}(\Omega X^{1+\varepsilon}b^{-1})$.

Let $\chi_0 := \overline{\chi}_1\chi_2$. The results of [Topacogullari 2018] cannot be quoted as a black box, however, the computations of [Topacogullari 2017] on which they are based may be adapted with little change. We write

$$\sum_{m_1,m_2} f(bm_1m_2)v_1\left(\frac{m_1}{M_1}\right)v_2\left(\frac{m_2}{M_2}\right)\chi_1(m_1)\chi_2(m_2)\tau(bm_1m_2-h) = \sum_{a \pmod D}\chi_1(a)D(a),$$

where $D(a)$ is the defined as

$$D(a) := \sum_n w_1\left(\frac{r_1n+f_1}{x_1}\right)w_2\left(\frac{r_2n+f_2}{x_2}\right)\tau(r_1n+f_1)\sum_{\substack{n_1,n_2\\ n_1n_2=r_2n+f_2}}\chi_0(n_2)h_{M_2M_1}(n_1,n_2),$$

with

$$r_1 := bD, \quad r_2 := D, \quad f_1 := ab - h, \quad f_2 := a, \quad x_1 := X, \quad x_2 := \frac{X}{b},$$

and

$$w_1(\xi) := \sqrt{f(X\xi + h)}, \quad w_2(\xi) := \sqrt{f(X\xi)}, \quad h_{M_2 M_1}(n_1, n_2) := v_2\Big(\frac{n_1}{M_2}\Big) v_1\Big(\frac{n_2}{M_1}\Big).$$

The sum $D(a)$ is now of the same shape as the sum $D_{AB}(x_1, x_2)$ defined in [Topacogullari 2017, page 157], with the function $\tilde{f}(a, b)$ there replaced by $\chi_0(a)\tilde{f}(a, b)$. The computations of Section 3 of [loc. cit.] can then be adapted with the following changes. In Section 3.1 of [loc. cit.] the expressions Σ^0_{AB} and $\Sigma^{\pm}_{AB}$ have an additional factor $\chi_0(au_2/u_2^*)$ in the summands. In the sums in the definition of $R^{\pm}_{AB}$, [loc. cit., page 159], the summand has to be multiplied by an additional factor $\chi_0(c)$, and the altered relation

$$\Sigma^{\pm}_{AB} = \sum_{\substack{u_2^* \mid u_2 \\ r_2^* \mid r_2}} \chi_0\Big(\frac{u_2}{u_2^*}\Big) \sum_{\substack{d \\ (d, r_1^* s_2 u_2^*)=1}} \chi_0(d) \frac{R^{\pm}_{AB}}{d}$$

holds. Consequently, the relationship between $R^{\pm}_{AB}(N; \chi)$ and $K^{\pm}_{AB}(N; \chi)$ becomes

$$R^{\pm}_{AB}(N; \chi) = \sum_{N < n \le 2N} \tau(n) \hat{S}_v(\bar{\chi}; n) K^{\pm}_{AB}(\chi\chi_0; n).$$

The rest of the argument of [loc. cit.] is adapted with the only change that the Kuznetsov formula is applied with nebentypus $\chi\chi_0$ instead of χ. This has no effect on the error terms, since the bounds in Theorem 2.6 and Lemmas 2.7, 2.8 and 2.9 of [loc. cit.] are uniform with respect to the nebentypus.

By the bound (3.4) of [loc. cit.], with $b^\circ = (b, D^\infty)$, $r_0 \leftarrow Db^\circ$ and $h \leftarrow hD$, we obtain

$$\begin{aligned} D(a) = \sum_{\substack{m_2 \\ (m_2, D)=1}} \frac{\chi_0(m_2) v_2\big(\frac{m_2}{M_2}\big)}{bDm_2} \sum_{d \mid bDm_2} \frac{c_d(abm_2\bar{m}_2 - h)}{d} \\ \times \int (\log(\xi - h) + 2\gamma - 2\log d) \cdot f(\xi) v_1\Big(\frac{\xi}{bM_1 m_2}\Big) d\xi \\ + \mathcal{O}\bigg(b^\circ D^{3/2} X^{1/2+\varepsilon}\bigg(\frac{1}{\Omega^{1/2}} + \Big(\frac{(b, h)X}{Db^2}\Big)^{\theta}\bigg\{1 + \Big(\frac{|h|}{bD}\Big)^{1/4}\bigg\}\bigg)\bigg), \end{aligned}$$

where $\bar{m}_2$ denotes any integer such that $\bar{m}_2 \cdot m_2 \equiv 1 \bmod D$. We sum over $a \pmod D$, exchange the a- and m_2-sums, and change variables $a \leftarrow am_2$. We obtain

$$\begin{aligned} &\sum_{a \pmod D} \chi_1(a) D(a) \\ &= \sum_{m_2} v\Big(\frac{m_2}{M_2}\Big) \chi_2(m_2) M^{\chi_1}_{f, v_1}(m_2 b, h; M_1) + \mathcal{O}\bigg(b^\circ D^{5/2} X^{1/2+\varepsilon}\bigg(\frac{1}{\Omega^{1/2}} + \Big(\frac{(b, h)X}{Db^2}\Big)^{\theta}\bigg\{1 + \Big(\frac{|h|}{bD}\Big)^{1/4}\bigg\}\bigg)\bigg), \end{aligned}$$

with $M^{\chi_1}_{f, v_1}(m_2 b, h; M_1)$ defined as in (4-4), for which we can use Lemma 4.3. The bound (4-11) follows after choosing $\Omega = X^{1/3}(M_1 M_2)^{-2/3}$. □

4E. *Type II estimates.* The following estimate, the first version of which was obtained in [Fouvry 1985], concerns convolutions with one component supported inside $[x^\varepsilon, x^{1/3-\varepsilon}]$.

Lemma 4.6. *For all $\eta, A > 0$, there exist $\delta, B > 0$ such that the following holds. Whenever $X, R \geq 1$, $(a, h) \in \mathbb{Z}^2$, an interval $I \subset [X/2, X]$, and two sequences (β_n), (γ_n) are given, under the conditions $1 \leq R, |a|, |h| \leq X^\delta$, and*

$$|\beta_n| \leq \tau_A(n), \quad |\gamma_n| \leq \tau_A(n), \quad \gamma_n \neq 0 \Longrightarrow n \in [X^\eta, X^{\frac{1}{3}-\eta}],$$

we have

$$\sum_{n \in I} (\beta * \gamma)(n) \Delta_h(an; R) \ll_{A,\eta} \tau((a,h)) R^{-1/2} X (\log X)^B. \tag{4-12}$$

Proof. Recall that $\Delta_h(an; R) \ll RX^\varepsilon$. In the left-hand side of (4-12), the contribution of those n such that $(n, (ah)^\infty) > X^\delta$ is therefore at most

$$RX^\varepsilon \sum_{\substack{n \ll X \\ (n,(ah)^\infty) > X^\delta}} 1 \ll RX^{1-\delta+\varepsilon}.$$

Next, we have

$$\sum_{\substack{d \mid (ah)^\infty \\ d \leq X^\delta}} \sum_{\substack{n \in I \\ d \mid n \\ (n/d, ah)=1}} (\beta * \gamma)(n) \Delta_h(an; R) = \sum_{\substack{\lambda_1,\lambda_2 \mid (ah)^\infty \\ \lambda_1\lambda_2 \leq X^\delta}} \sum_{\substack{mn \in (\lambda_1\lambda_2)^{-1} I \\ (mn, ah)=1 \\ (m,\lambda_2)=1}} \beta_{\lambda_1 m} \gamma_{\lambda_2 n} \Delta_h(a\lambda_1\lambda_2 mn; R).$$

Finally, we note that there are at most $\mathcal{O}(X^{1/2+\varepsilon})$ tuples $(\lambda_1, \lambda_2, m, n)$ with $\lambda_1\lambda_2 mn \in I$ for which the expression $a\lambda_1\lambda_2 mn - h$ is a perfect square, and

$$\Delta_h(a\lambda_1\lambda_2 mn; R) = 2 \sum_{\lambda_3 \mid (h, a\lambda_1\lambda_2)} \sum_{\substack{q \leq \sqrt{a\lambda_1\lambda_2 mn - h}/\lambda_3 \\ (q, a\lambda_1\lambda_2 h/\lambda_3^2)=1}} \mathfrak{u}_R\Big(mn \tfrac{a\lambda_1\lambda_2}{\lambda_3} \tfrac{\overline{h}}{\lambda_3}; q\Big) + \mathcal{O}(\mathbf{1}_{a\lambda_1\lambda_2 mn - h \text{ is a square}}),$$

where the notation $\mathfrak{u}_R(n; q)$ is defined in formula (5.1) of [Drappeau 2017]. Now, for each $(\lambda_1, \lambda_2, \lambda_3)$, the sum

$$S(\lambda_1, \lambda_2, \lambda_3) = \sum_{\substack{q \leq \sqrt{a\lambda_1\lambda_2 mn - h}/\lambda_3 \\ (q, a\lambda_1\lambda_2 h/\lambda_3^2)=1}} \sum_{\substack{mn \in (\lambda_1\lambda_2)^{-1} I \\ (mn, ah)=1 \\ (m,\lambda_2)=1}} \mathfrak{u}_R\Big(mn \tfrac{a\lambda_1\lambda_2}{\lambda_3} \tfrac{\overline{h}}{\lambda_3}; q\Big)$$

is of the same shape as in formula (5.6) of [Drappeau 2017], with three differences:

(1) The quantity $\tau_A(\lambda_1)\tau_A(\lambda_2)$ has to be factored out for the condition (5.4) of [loc. cit.] to hold.

(2) The sums over m and n must be restricted to dyadic intervals, which is done at the cost of an additional factor $(\log x)^2$.

(3) The sums over m, n and q are not separated.

The last point can be implemented by a standard argument (see e.g., page 720 of [loc. cit.]), cutting the (m, n) sums into intervals of type $[M, (1+\xi)M] \times [N, (1+\xi)N]$ with $\xi \asymp R^{-1/2}$. Assuming δ is small enough in terms of η, we obtain

$$\begin{aligned} S(\lambda_1, \lambda_2, \lambda_3) &\ll \tau_A(\lambda_1)\tau_A(\lambda_2)(\lambda_1\lambda_2)^{-1} X(\log X)^B(\xi + \xi^{-1}R^{-1}) \\ &\ll \tau_A(\lambda_1)\tau_A(\lambda_2)(\lambda_1\lambda_2)^{-1} R^{-1/2} X(\log X)^B. \end{aligned}$$

We sum this over $(\lambda_1, \lambda_2, \lambda_3)$ satisfying

$$\lambda_1\lambda_2 \mid (ah)^\infty, \quad \lambda_1\lambda_2 \le x^\delta, \quad \lambda_3 \mid (h, a\lambda_1\lambda_2).$$

Since $\sum_{\lambda \mid (ah)^\infty} \tau_{2A}(\lambda)\tau(\lambda)\lambda^{-1} \ll_A (\log\log x)^{O_A(1)}$, we obtain

$$\sum_{n \in I} (\beta * \gamma)(n)\Delta_h(an; R) \ll \tau((a, h))\{RX^{1-\delta/2} + R^{-1/2}X(\log X)^{B+1}\},$$

which yields our claim by reinterpreting δ and B. □

5. The case of rational parameters

Let $\chi_1, \dots, \chi_T$ be distinct Dirichlet characters mod D, and the function $f \in \mathcal{F}_D^{\tau_\mathbb{Q}}(A)$ be defined by

$$\sum_{n=1}^{\infty} \frac{f(n)}{n^s} := \prod_{j=1}^{T} L(s, \chi_j)^{b_j}, \tag{5-1}$$

with $b_1, \dots, b_T \in \mathbb{Q}$, which we write in the form

$$b_j = r_j + \frac{u_j}{v_j} \quad \text{with } r_j \in \mathbb{Z} \text{ and } u_j, v_j \in \mathbb{N} \text{ such that } 0 \le u_j < v_j.$$

For notational convenience we also define

$$\|r\|_1 := \sum_{1 \le j \le T} |r_j|, \quad \|v\|_1 := \sum_{1 \le j \le T} v_j.$$

Our goal is to prove estimate (2-4) for the function f defined in (5-1). In fact, we will prove a result which is slightly more precise in term of uniformity in D and T.

Proposition 5.1. *Let $A, D, T \ge 1$ be fixed. Then we have, for $x \ge 3$, $I \subset [x/2, x]$ and $f \in \mathcal{F}_D^{\tau_\mathbb{Q}}(A)$ as described above, the following estimate,*

$$|\Sigma_f(I; a, h; R)| \le C\tau((a, h))D^{5/2}\frac{x(\log x)^{B+\omega(D)}}{R^{1/2}}\|v\|_1 \quad \text{for } 1 \le a, |h|, R \le x^\delta, \tag{5-2}$$

where $\delta > 0$ is some absolute constant, and where $B, C > 0$ are constants which depend only on A and T.

The rest of this section is now concerned with proving Proposition 5.1.

5A. *Application of the combinatorial identity.* Denote $\tau_z^{\chi}(n) := \tau_z(n)\chi(n)$, so that

$$f(n) = \tau_{b_1}^{\chi_1} * \cdots * \tau_{b_T}^{\chi_T}. \tag{5-3}$$

The expression on the left-hand side of (5-2) now reads

$$\Sigma_f(I; a, h; R) = \sum_{m_1 \cdots m_T \in I} \tau_{b_1}^{\chi_1}(m_1) \cdots \tau_{b_T}^{\chi_T}(m_T) \Delta_h(am_1 \cdots m_T; R). \tag{5-4}$$

By Theorem 3.2 with $K = 4$ we can write $\tau_{b_j}^{\chi_j}(m_j)$ as

$$\tau_{b_j}^{\chi_j}(m_j) = \sum_{\ell=1}^{4} c_{\ell,j} \sum_{\substack{m_1 \cdots m_{k_{\ell,j}} n_1 \cdots n_{k'_{\ell,j}} = m_j \\ n_1, \ldots, n_{k'_{\ell,j}} \le x^{1/4}}} \!\!\cdots\!\! \sum \chi_j(m_1) \cdots \chi_j(m_{k_{\ell,j}}) \tau_{-1/v_j}^{\chi_j}(n_1) \cdots \tau_{-1/v_j}^{\chi_j}(n_{k'_{\ell,j}}), \tag{5-5}$$

where $(k_{\ell,j})_{\ell=1}^{4}$ and $(k'_{\ell,j})_{\ell=1}^{4}$ are two sequences of integers satisfying

$$0 \le k_{\ell,j} \le |r_j| + 4, \quad 1 \le k'_{\ell,j} \le (|r_j| + 4)v_j,$$

and where $(c_{\ell,j})_{\ell=1}^{4}$ is a set of complex numbers whose moduli are bounded in terms of A. We replace each factor $\tau_{b_j}^{\chi_j}(m_j)$ in (5-4) by its decomposition, and after expanding the resulting expression, we end up with a linear combination (whose coefficients are bounded by $\mathcal{O}_A(1)$) of $\mathcal{O}_T(1)$ sums of the form

$$\Xi := \sum_{\substack{m_1 \cdots m_k n_1 \cdots n_{k'} \in I \\ n_1, \ldots, n_{k'} \le x^{1/4}}} \sigma_1(m_1) \cdots \sigma_k(m_k) \varrho_1(n_1) \cdots \varrho_{k'}(n_{k'}) \Delta(am_1 \cdots m_k n_1 \cdots n'_k; R), \tag{5-6}$$

where each function σ_i is some Dirichlet character mod D, where each function ϱ_i is equal to $\tau_{-1/v_j}^{\chi_j}$ for some j, and where k and k' are integers bounded by

$$0 \le k \le 4T + \|r\|_1 \quad \text{and} \quad 1 \le k' \le 4\|v\|_1 + \sum_{1 \le j \le T} |r_j| v_j.$$

We consider each sum Ξ separately.

For technical reasons, it will be necessary to use a smooth dyadic decomposition for the variables $m_1, \ldots, m_k$. Let $u : (0, \infty) \to \mathbb{R}$ be a smooth and compactly supported function, which satisfies

$$\operatorname{supp} u \subset \left[\tfrac{1}{4}, 2\right] \quad \text{and} \quad \sum_{\ell \in \mathbb{Z}} u\left(\frac{\xi}{2^\ell}\right) = 1 \quad \text{for all } \xi \in (0, \infty),$$

and define

$$u_0(\xi) := \sum_{\ell \le 0} u\left(\frac{\xi}{M_\ell}\right) \quad \text{and} \quad u_\ell(\xi) := u\left(\frac{\xi}{M_\ell}\right) \quad \text{for } \ell > 0,$$

where we have set

$$M_\ell := x^{1/4+\eta} 2^\ell,$$

with $0 < \eta < \frac{1}{24}$ an arbitrary, but fixed constant. For a k-tuple $\ell = (\ell_1, \dots, \ell_k) \in \mathbb{N}^k$, we then define

$$\Xi_\ell := \sum_{\substack{m_1 \cdots m_k n_1 \cdots n_{k'} \in I \\ n_1, \dots, n_{k'} \le x^{1/4}}} u_{\ell_1}(m_1)\sigma_1(m_1) \cdots u_{\ell_k}(m_k)\sigma_k(m_k)\varrho_1(n_1) \cdots \varrho_{k'}(n_{k'})\Delta(am_1 \cdots m_k n_1 \cdots n'_k; R),$$

so that the sum Ξ can be split as

$$\Xi = \sum_{\ell \in \mathbb{N}^k} \Xi_\ell.$$

Note that this last sum is in fact finite, since Ξ_ℓ becomes empty if the coordinates of ℓ are large enough, namely if $\ell_1, \dots, \ell_k \gg \log x$. We will now estimate the sums Ξ_ℓ in different ways, depending on the sizes of the supports of the variables m_i.

5B. ***Case I.*** First assume that ℓ has at least one coordinate, say ℓ_1, satisfying $M_{\ell_1} \ge x^{1/3+\eta}$. Let $m_0 := m_2 \cdots m_k n_1 \cdots n_{k'}$. Denoting $\sigma_1 = \chi_j$ for some j, we can use Lemma 4.4 with $X = ax$, $b = am_0$ and $M = M_{\ell_1}$ to get

$$\sum_{m_1 : m_0 m_1 \in I} u_{\ell_1}(m_1)\sigma_1(m_1)\Delta_h(am_0m_1; R) \ll_{\varepsilon, A} x^\varepsilon \biggl(Da^{1/3}x^{1/3} + (am_0, hD^\infty)\frac{M_{\ell_1}}{x^{1/2}} + D^{1/2}R^{3/2} \biggr).$$

This leads to

$$\Xi_\ell \ll_\varepsilon x^\varepsilon (Da^{1/3}x^{1-\eta} + (a, hD^\infty)(\log x)^{\omega(D)}x^{1/2} + x^{2/3-\eta}D^{1/2}R^{3/2}), \tag{5-7}$$

where we have made use of the fact that

$$\sum_{m_0 \le x/M_{\ell_1}} (m_0, hD^\infty) \le \sum_{\substack{D^* \mid D^\infty \\ D^* \le x}} D^* \sum_{m_0 \le x/(D^* M_{\ell_1})} (m_0, h) \ll_\varepsilon h^\varepsilon \frac{x}{M_{\ell_1}} \sum_{\substack{D^* \mid D^\infty \\ D^* \le x}} 1 \ll_\varepsilon \frac{(\log x)^{\omega(D)} x^{1+\varepsilon}}{M_{\ell_1}}.$$

5C. ***Case II.*** Next assume that ℓ has at least two nonzero coordinates, say $\ell_1 \ge \ell_2 \ge 1$. We can also assume that $x^{1/4+\eta} \ll M_{\ell_1}, M_{\ell_2} \ll x^{1/3+\eta}$, since the case of larger M_{ℓ_1} and M_{ℓ_2} is already treated above. Let $m_0 := m_3 \cdots m_k n_1 \cdots n_{k'}$. We use Lemma 4.5 with $X = ax$ and $b = am_0$, which gives

$$\sum_{\substack{m_1, m_2 : \\ m_0 m_1 m_2 \in I}} u_{\ell_1}(m_1)\sigma_1(m_1)u_{\ell_1}(m_1)\sigma_2(m_2)\Delta_h(am_0m_1m_2; R)$$

$$\ll_{\varepsilon, A} (am_0, D^\infty)x^\varepsilon \biggl(D^{5/2}(axM_{\ell_1}M_{\ell_2})^{1/3} + (h, am_0)R^{3/2}\frac{M_{\ell_1}M_{\ell_2}}{a^{1/2}x^{1/2}} \biggr),$$

so that altogether we are led to

$$\Xi_\ell \ll_{\varepsilon, A} (a, h)(a, D^\infty)(\log x)^{\omega(D)}x^\varepsilon (D^{5/2}a^{1/3}x^{1-4/3\eta} + (a, h)R^{3/2}x^{1/2}). \tag{5-8}$$

5D. ***Case III.*** Finally, we need to consider the case, where ℓ has at most one nonzero coordinate, say ℓ_1, for which we have $M_{\ell_1} \ll x^{\frac{1}{3}+\eta}$. We split the sum Ξ_ℓ into two parts,

$$\Xi_j =: \Xi_\ell^{(1)} + \Xi_\ell^{(2)},$$

according to whether $n_1 \cdots n_{k'} > x^\eta$ or $n_1 \cdots n_{k'} \le x^\eta$.

We look first at $\Xi_\ell^{(1)}$. We split this sum according to the value of

$$\mu = \min\{1 \le \mu' \le k' : \ n_1 \cdots n_{\mu'} > x^\eta\},$$

and write accordingly

$$\Xi_\ell^{(1)} =: \sum_{\mu=1}^{k'} \Xi_\ell^{(1)}(\mu).$$

After defining

$$\beta_m := \sum_{\substack{m_1 \cdots m_k n_{\mu+1} \cdots n_{k'} = m \\ n_{\mu+1}, \ldots, n_{k'} \le x^{1/4}}} u_{\ell_1}(m_1)\sigma_1(m_1) \cdots u_0(m_k)\sigma_k(m_k)\varrho_{\mu+1}(n_{\mu+1}) \cdots \varrho_{k'}(n_{k'}),$$

and

$$\gamma_n := \sum_{\substack{n_1 \cdots n_\mu = n \\ n_1 \cdots n_{\mu-1} \le x^\eta, n_1, \ldots, n_\mu \le x^{1/4}}} \varrho_1(n_1) \cdots \varrho_\mu(n_\mu),$$

and renaming $n \leftarrow n_1 \cdots n_\mu$ and $m \leftarrow m_1 \cdots m_k n_{\mu+1} \cdots n_{k'}$, we can write $\Xi_\ell^{(1)}(\mu)$ as

$$\Xi_\ell^{(1)}(\mu) = \sum_{\substack{m,n:\ mn \in I \\ x^\eta < n \le x^{1/4+\eta}}} \beta_m \gamma_n \Delta_h(amn; R).$$

Note that $\gamma_n = 0$ if $n > x^{1/4+\eta}$. Moreover, we can bound the quantities β_m and γ_n by

$$|\beta_m| \le \tau_{2\|r\|_1+8T}(m), \quad |\gamma_n| \le \tau_{\|r\|_1+4T}(n).$$

Hence we can apply Lemma 4.6 with $A \leftarrow 2\|r\|_1 + 8T$, and we see that

$$\Xi_\ell^{(1)}(\mu) \ll \tau((a,h)) R^{-1/2} x (\log x)^{B_1} \quad \text{for } 1 \le a, |h|, R \le x^{\delta_1},$$

where $\delta_1, B_1 > 0$ are certain constants which depend solely on η and A. Summing over μ, we deduce

$$\Xi_\ell^{(1)} \ll_A \tau((a,h)) R^{-1/2} x (\log x)^{B_1} \|v\|_1 \quad \text{for } 1 \le a, |h|, R \le x^{\delta_1}. \tag{5-9}$$

The other sum $\Xi_\ell^{(2)}$ can be estimated similarly — the role of the variables $n_1, \ldots, n_{k'}$ is now played by the variables $m_2, \ldots, m_k$. Eventually, we get

$$\Xi_\ell^{(2)} \ll_A \tau((a,h)) R^{-1/2} x (\log x)^{B_2} \quad \text{for } 1 \le a, |h|, R \le x^{\delta_2}, \tag{5-10}$$

where $\delta_2, B_2 > 0$ are certain constants which again depend solely on η and A.

5E. *Conclusion.* Grouping the different bounds (5-7)–(5-10), setting $B := \max(B_1, B_2)$ and choosing $\delta > 0$ small enough, we get

$$\Xi \ll \tau((a,h)) D^{5/2} R^{-1/2} x (\log x)^{B+\omega(D)} \|v\|_1 \quad \text{for } 1 \le a, |h|, R \le x^{\delta},$$

with the implicit constant depending only on A and T. This finally proves Proposition 5.1.

6. Interpolation to complex parameters

Let $r_1, \dots, r_{\varphi(D)}$ be the residues mod D which are relatively prime to D. Any $f \in \mathcal{F}_D^{\omega}(A)$ is given by

$$\sum_{n=1}^{\infty} \frac{f(n)}{n^s} = \prod_{j=1}^{\varphi(D)} \prod_{p \equiv r_j \bmod D} \left(1 + \frac{z_j}{p^s - 1}\right), \tag{6-1}$$

for $\mathbf{z} = (z_1, \dots, z_{\varphi(D)}) \in \mathbb{C}^{\varphi(D)}$, with $|z_j| \le A$. After setting

$$\omega_r(n) := \#\{p \text{ prime} : p \mid n,\, p \equiv r \bmod D\}, \tag{6-2}$$

we can also write

$$f(n) = \sum_{n_1 \cdots n_{\varphi(D)} = n} \prod_{j=1}^{\varphi(D)} z_j^{\omega_{r_j}(n_j)}.$$

Our aim here is to show that the bound (2-4) holds for $\Sigma_f(I; a, h; R)$, for all $f \in \mathcal{F}_D^{\omega}(A)$. By Lemma 2.5 this will imply Proposition 2.1.

Let $\chi_1, \dots, \chi_{\varphi(D)}$ be the Dirichlet characters mod D, let Q be the unitary matrix

$$Q := \frac{1}{\sqrt{\varphi(D)}} \begin{pmatrix} \chi_1(r_1) & \chi_2(r_1) & \cdots & \chi_{\varphi(D)}(r_1) \\ \chi_1(r_2) & \chi_2(r_2) & \cdots & \chi_{\varphi(D)}(r_2) \\ \vdots & \vdots & \ddots & \vdots \\ \chi_1(r_{\varphi(D)}) & \chi_2(r_{\varphi(D)}) & \cdots & \chi_{\varphi(D)}(r_{\varphi(D)}) \end{pmatrix},$$

and let $M_Q : \mathbb{C}^{\varphi(D)} \to \mathbb{C}^{\varphi(D)}$ be the bijective linear map associated to Q.

Let $K \ge 1$. We define $\mathcal{F}_D^{\omega}(A, K)$ to be the set of functions $f \in \mathcal{F}_D^{\omega}(A)$ of the same form as in (6-1), but with the additional property that the parameters $\mathbf{z}$ are given by

$$\mathbf{z} = M_Q(\boldsymbol{b})$$

for a tuple of rational numbers $\boldsymbol{b} = (b_1, \dots, b_{\varphi(D)}) \in \mathbb{Q}^{\varphi(D)}$ satisfying

$$|b_j| \le A \quad \text{and} \quad b_j = \frac{u_j}{v_j} \quad \text{with } u_j, v_j \in \mathbb{Z} \text{ and } |v_j| \le K,$$

for all $j = 1, \dots, \varphi(D)$. By Proposition 5.1, Lemma 2.2 and Lemma 2.3, we deduce that the bound (2-4) holds for all $f \in \mathcal{F}_D^{\omega}(A, K)$ in the following form.

Proposition 6.1. *Let $A, D \geq 1$ be fixed. For $K \geq 1$, $x \geq 3$, $I \subset [x/2, x]$ and $f \in \mathcal{F}_D^{\omega}(A, K)$, we have*

$$|\Sigma_f(I; a, h; R)| \leq C K \tau((a, h)) \frac{x(\log x)^B}{R^{1/2}} \quad \text{for } 1 \leq a, |h|, R \leq x^{\delta}, \tag{6-3}$$

where $\delta > 0$ is some absolute constant, and where $B, C > 0$ are constants which depend only on A and D.

Our goal is to interpolate this result to all functions in $\mathcal{F}_D^{\omega}(A)$. Let $f \in \mathcal{F}_D^{\omega}(A)$ be fixed, with $\mathbf{z}$ as in (6-1). For $L \in [1, \infty]$, we define two polynomials in the variables $\mathbf{Z} = (Z_1, \ldots, Z_{\varphi(D)})$ as follows,

$$P_L(\mathbf{Z}) := \sum_{\substack{n \in I \\ \forall j, \omega_{r_j}(n) \leq L}} \sum_{n_1 \cdots n_{\varphi(D)} = n} \prod_{j=1}^{\varphi(D)} Z_j^{\omega_{r_j}(n_j)} \Delta_h(an; R), \quad \tilde{P}_L(\mathbf{Z}) := P_L(M_Q(\mathbf{Z})).$$

By definition, both these polynomials have degree at most L in each variable. Furthermore, let

$$\boldsymbol{b} := M_Q^{-1}(\mathbf{Z}),$$

and note that $\|\boldsymbol{b}\|_\infty \leq D^{1/2} A$. Using this notation, we can now write the sum $\Sigma_f(I; a, h; R)$ simply as

$$\sum_{n \in I} f(n) \Delta_h(an; R) = \tilde{P}_\infty(\boldsymbol{b}).$$

In order to have better control over the degree of $\tilde{P}_\infty(\mathbf{Z})$, we cut off all the terms of degree larger than some fixed real number $L \geq 1$. For a tuple $\zeta = (\zeta_1, \ldots, \zeta_{\varphi(D)})$ satisfying $|\zeta_j| \leq A D^{1/2}$ and any real number $E \geq 1$, this leads to an error term of the following form,

$$\begin{aligned}
|\tilde{P}_\infty(\zeta) - \tilde{P}_L(\zeta)| &\leq \sum_{\substack{n \in I \\ \omega(n) > L}} \tau_D(n)(AD)^{\omega(n)} |\Delta_h(an; R)| \\
&\leq E^{-L} \sum_{n \leq x} \tau_D(n)(ADE)^{\omega(n)} |\Delta_h(an; R)| \\
&\leq E^{-L} \Bigl(\sum_{n \leq x} \tau_{AD^2E}(n)^2\Bigr)^{1/2} \Bigl(\sum_{n \leq x} |\Delta_h(an; R)|^2\Bigr)^{1/2}.
\end{aligned}$$

The different factors can be estimated via [Tenenbaum 1995, Theorem II.6.1], and Lemma 4.1, and we get

$$\begin{aligned}
|\tilde{P}_\infty(\zeta) - \tilde{P}_L(\zeta)| &\ll E^{-L} (x(\log x)^{(ADE)^4 - 1})^{1/2} (x(\log x)^4 \tau((a, h))^2)^{1/2} \\
&\ll E^{-L} \tau((a, h)) x (\log x)^{(ADE)^4/2 + 2},
\end{aligned} \tag{6-4}$$

where the implicit constants depend at most on A, E and D.

Next, we set

$$\beta_\ell := \frac{2(\ell + 1)\lfloor AD^{1/2} \rfloor}{L + 1} - \lfloor AD^{1/2} \rfloor \quad \text{for } \ell = 0, \ldots, L.$$

Obviously, all these numbers are bounded by $|\beta_\ell| \le AD^{1/2}$, and are rational numbers with denominators not larger than $L+1$. Furthermore, we have the bound

$$|\beta_{\ell_1} - \beta_{\ell_2}| \ge \frac{AD^{1/2}}{2L} |\ell_1 - \ell_2| \quad \text{for } \ell_1 \ne \ell_2.$$

For any tuple $\ell = (\ell_1, \dots, \ell_{\varphi(D)}) \in \{0, \dots, L\}^{\varphi(D)}$, denote $\beta_\ell = (\beta_{\ell_1}, \dots, \beta_{\ell_{\varphi(D)}})$. The value $\tilde{P}_\infty(\beta_\ell)$ can be interpreted as an instance of the sum $\Sigma_{\tilde{f}}(I; a, h; R)$ for an appropriate function $\tilde{f} \in \mathcal{F}_D^\omega(AD, L+1)$,

$$\tilde{P}_\infty(\beta_\ell) = \Sigma_{\tilde{f}}(I; a, h; R).$$

Hence, by Proposition 6.1 and the estimate in (6-4) we can deduce

$$\tilde{P}_L(\beta_\ell) \ll_{A,D} \tau((a,h)) x (\log x)^{(ADE)^4/2+B} \left(\frac{L}{R^{1/2}} + \frac{1}{E^L} \right), \tag{6-5}$$

uniformly for $1 \le a, |h|, R \le x^\delta$.

By Lagrange interpolation, we bring $\tilde{P}_L(\boldsymbol{b})$ into the following shape,

$$\tilde{P}_L(\boldsymbol{b}) = \sum_{\ell \in \{0,\dots,L\}^{\varphi(D)}} \tilde{P}_L(\beta_\ell) \prod_{j=1}^{\varphi(D)} \prod_{\substack{0 \le i \le L \\ i \ne \ell_j}} \frac{b_j - \beta_i}{\beta_{\ell_j} - \beta_i},$$

which is allowed since the Vandermonde determinant associated to (β_ℓ) does not vanish. We can now estimate $\tilde{P}_L(\boldsymbol{b})$ via the already known bound (6-5) for the expressions $\tilde{P}_L(\beta_\ell)$. Namely, we have

$$\begin{aligned} |\tilde{P}_L(\boldsymbol{b})| &\le \sum_{\ell \in \{0,\dots,L\}^{\varphi(D)}} |\tilde{P}_L(\beta_\ell)| \prod_{j=1}^{\varphi(D)} \prod_{\substack{0 \le i \le L \\ i \ne \ell_j}} \frac{|b_j - \beta_i|}{|\beta_{\ell_j} - \beta_{\ell_i}|} \\ &\ll \tau((a,h)) x (\log x)^{(ADE)^4/2+B} \left(\frac{L}{R^{1/2}} + \frac{1}{E^L} \right) (4L)^{L\varphi(D)} \sum_{\ell \in \{0,\dots,L\}^{\varphi(D)}} \prod_{j=1}^{\varphi(D)} \prod_{\substack{0 \le i \le L \\ i \ne \ell_j}} \frac{1}{|\ell_j - i|} \\ &\ll \tau((a,h)) x (\log x)^{(ADE)^4/2+B} \left(\frac{L}{R^{1/2}} + \frac{1}{E^L} \right) \frac{(8L)^{L\varphi(D)}}{(L!)^{\varphi(D)}}, \end{aligned}$$

which after using Stirling's approximation for the gamma function simplifies to

$$|\tilde{P}_L(\boldsymbol{b})| \ll \tau((a,h)) x (\log x)^{(ADE)^4/2+B} \left(\frac{1}{R^{1/2}} + \frac{1}{E^L} \right) (4e)^{2DL},$$

with the implicit constant depending at most on A, E and D.

After adding all the terms we had cut off earlier, we are finally led to

$$\Sigma_f(I; a, h; R) \ll_{A,D,E} \tau((a,h)) x (\log x)^{(ADE)^4/2+B} \left(\frac{1}{R^{1/2}} + \frac{1}{E^L} \right) (4e)^{2DL}.$$

With the choices

$$L := \frac{\log R}{12D\log(4e)} \quad \text{and} \quad E := (4e)^{6D},$$

and after reinterpreting the constant B, we get

$$\Sigma_f(I; a, h; R) \ll_{A,D} \tau((a,h))\frac{x(\log x)^B}{R^{1/3}} \quad \text{for } 1 \le a, |h|, R \le x^{\delta},$$

which is exactly the statement we wanted to prove.

7. Proof of Theorem 1.2 using Linnik's identity

We now sketch how Theorem 1.2 can alternatively be proven using Theorem 3.3. The details of the computations being very similar, we will restrict to discussing the main differences in the arguments.

As mentioned above, it is enough to consider the case $f \in \mathcal{F}_D^{\tau}(A)$, or in other words we can assume that $f = \tau_{b_1}^{\chi_1} * \cdots * \tau_{b_T}^{\chi_T}$, where $\chi_1, \ldots, \chi_T$ are distinct Dirichlet characters mod D, and where $b_1, \ldots, b_T$ are complex numbers whose moduli are bounded by A. The sum in consideration is then given by

$$\Sigma_f(I; a, h; R) = \sum_{m_1 \cdots m_T \in I} \tau_{b_1}^{\chi_1}(m_1) \cdots \tau_{b_T}^{\chi_T}(m_T)\Delta_h(am_1 \cdots m_T; R).$$

Here we replace each $\tau_{b_j}^{\chi_j}(m_j)$ by its decomposition as given in Theorem 3.3 with $K = 4$, and after expanding the resulting expression, we end up with a linear combination of sums of the form

$$\Xi := \sum_{\substack{m_1 \cdots m_k n_1 \cdots n_T \in I \\ P^+(n_1 \cdots n_T) \le x^{1/4}}} \sigma_1(m_1) \cdots \sigma_k(m_k)\rho_1(n_1) \cdots \rho_T(n_T)\Delta(am_1 \cdots m_k n_1 \cdots n_T; R),$$

where each function σ_j is some Dirichlet character mod D, where each function ρ_j is equal to $\tau_{b_j-\ell}^{\chi_j}$ for some j and $\ell \in [0, 3]$, and where $k \le 3T$. We consider each sum Ξ separately.

To each factor ρ_j in the sum Ξ we apply Lemma 3.4 with $y = x^{1/4}$ and $w = x^{\eta}$ for some arbitrary, but fixed $\eta \in \left(0, \frac{1}{24}\right)$. By compacity, it follows that for each $j = 1, \ldots, T$ there exist arithmetic functions α_j and β_j, such that the sum Ξ can be written as

$$\Xi = \sum_{j=1}^{T} \Xi_j^{(1)} + \sum_{j=1}^{T} \Xi_j^{(2)} + \Xi^{(3)},$$

with

$$\Xi_j^{(1)} := \sum_{\substack{mn_1 \cdots n_T \in I \\ P^+(n_1 \cdots n_T) \le x^{1/4} \\ n_1, \ldots, n_{j-1} \le x^{\eta}, n_j > x^{1/\eta} \\ \exists p^k \parallel n_j, p^k > x^{1/4}}} (\sigma_1 * \cdots * \sigma_k)(m)\rho_1(n_1) \cdots \rho_T(n_T)\Delta(amn_1 \cdots n_T; R),$$

$$\Xi_j^{(2)} := \sum_{\substack{mn_1\cdots n_{j_1}n_j'n_j''n_{j+1}\cdots n_T\in I \\ P^+(n_1\cdots n_{j_1}n_j'n_j''n_{j+1}\cdots n_T)\le x^{1/4} \\ n_1,\dots,n_{j-1}\le x^\eta,\, x^\eta<n_j'\le x^{1/4+\eta}}} (\sigma_1*\cdots*\sigma_k)(m)\Bigl(\prod_{\substack{1\le k\le T\\ k\ne j}}\rho_k(n_k)\Bigr)\alpha_j(n_j')\beta_j(n_j'')\Delta(amn_1\cdots n_T;\, R),$$

$$\Xi^{(3)} := \sum_{\substack{mn_1\cdots n_T\in I \\ n_1,\dots,n_T\le x^\eta}} (\sigma_1*\cdots*\sigma_k)(m)\rho_1(n_1)\cdots\rho_T(n_T)\Delta(amn_1\cdots n_T;\, R).$$

The sums $\Xi_j^{(1)}$ can be bound trivially. Indeed, we note that if a prime power $p^k > y$ divides n, then since $P^+(n_j)\le y$ we must have $k\ge 2$. Hence

$$\begin{aligned}\Xi_j^{(1)} &\le \sum_{\substack{n\in I\\ \exists p^k\,|\,n:\,p^k>x^{1/4},\ k\ge 2}} \tau_{(A+6)T}(n)|\Delta(an;\,R)| \\ &\ll_\varepsilon \Bigl(\sum_{n\in I}|\Delta(an;\,R)|^2\Bigr)^{1/2}\Bigl(\sum_{\substack{n\in I\\ \exists p^k\,|\,n:\,p^k>x^{1/4},\ k\ge 2}} 1\Bigr)^{1/2} \\ &\ll_{A,T} x^{1-1/17}\tau((a,h)),\end{aligned}$$

which is an acceptable error term.

Concerning the sums $\Xi_j^{(2)}$, we can bound them following the arguments of Case III, Section 5D, since we have a variable localized in $[x^\eta, x^{1/4+\eta}]$, and since $\frac{1}{4}+\eta<\frac{1}{3}$. The remaining sum $\Xi^{(3)}$, which is analogous to (5-6), can be estimated for all sufficiently small $\eta>0$ by the arguments of Sections 5B, 5C and 5D, according to the size of the involved variables. As a result, we get for these sums the estimate

$$\Xi_j^{(2)},\ \Xi^{(3)} \ll_{A,T} \tau((a,h))\frac{x(\log x)^{\mathcal{O}(1)}}{R^{1/2}}.$$

Together with the bound for $\Xi_j^{(1)}$, this eventually proves Theorem 1.2.

8. Proof of Theorems 1.2, 1.3, 1.4 and 1.6

In this section we want to deduce Theorem 1.2 from Proposition 2.1, and afterwards apply this result to the problems mentioned in the introduction. Before doing so, we first need to prove an auxiliary result, which is concerned with bounds on average for functions in $\mathcal{F}_D(A)$ twisted by a Dirichlet character.

Lemma 8.1. *Let $f\in\mathcal{F}_D(A)$ and let $B\ge 1$. Then there exists a constant $c>0$, such that, for all Dirichlet characters χ mod q satisfying $\operatorname{cond}(\chi)\nmid D$ and $q\le(\log x)^B$, we have*

$$\sum_{n\le x}\chi(n)f(n)\ll xe^{-c\sqrt{\log x}}. \tag{8-1}$$

Both the constant c and the implicit constant depend at most on A, B and D.

Proof. Let $F_\chi(s)$ be the Dirichlet series associated to the function $\chi(n)f(n)$. By Lemma 2.4 we know that $F_\chi(s)$ can be written as

$$F_\chi(s) = H_\chi(s) \prod_{\psi \bmod D} L(s, \chi\psi)^{b_\psi} \quad \text{for } \mathfrak{Re}(s) > 1,$$

where $H_\chi(s)$ is a holomorphic function in $\mathfrak{Re}(s) \geq \frac{1}{2} + \varepsilon$, bounded in terms of A, D only.

Due to the assumption $\operatorname{cond}(\chi) \nmid D$ we know that none of the characters $\chi\psi$ is principal, which means that none of the L-functions $L(s, \chi\psi)$ has a pole at $s = 1$. It follows from Siegel's theorem that for any $\delta > 0$ there exists a constant $c(\delta)$ such that all $L(s, \chi\psi)$ are zero-free in the region defined by the condition $\mathfrak{Re}(s) > 1 - \gamma(\mathfrak{Im}(s))$, where

$$\gamma(t) := \min\left\{ \frac{c(\delta)}{\log(qD(|t|+2))}, \frac{c(\delta)}{(qD)^\delta} \right\}. \tag{8-2}$$

Using this zero-free region, the bound (8-1) follows using a standard contour integration argument; see e.g., [Montgomery and Vaughan 2007, Section 11.3]. □

We now proceed to prove Theorem 1.2. We set $R = (\log x)^L$ where $L \geq 1$ is some constant which depends only on A, B and D, and which we will determine at the very end. Note that in any case we can assume x to be large enough so that $D \leq R$ is satisfied.

We start by splitting the sum $D_f(x; a, h)$ into two parts as follows,

$$D_f(x; a, h) = D_f(\sqrt{x}; a, h) + \sum_{\sqrt{x} < n \leq x} f(n)\tau(an - h).$$

While the first sum can be estimated by trivial means, we can use Proposition 2.1 to evaluate the second (after first dividing the range of summation into dyadic intervals). This eventually shows that there exists an absolute constant $\delta > 0$, and a constant B depending only on A and D, such that, for all $1 \leq a, |h| \leq x^\delta$,

$$D_f(x; a, h) = \tilde{M}_f(x; a, h) + \mathcal{O}\left(\tau((a, h)) \frac{x(\log x)^B}{R^{1/3}} \right),$$

with

$$\tilde{M}_f(x; a, h) := \sum_{|h|/a < n \leq x} f(n)\tilde{\tau}_h(an; R).$$

It remains to evaluate this last sum.

After expanding $\tilde{\tau}_h(an; R)$, it can be written as

$$\tilde{M}_f(x; a, h) = 2 \sum_{q \leq \sqrt{ax}} \frac{1}{\varphi\left(\frac{q}{(h,q)}\right)} \sum_{\substack{\chi \bmod q/(h,q) \\ \operatorname{cond} \chi \leq R}} \bar{\chi}\left(\tfrac{h}{(h,q)}\right) \sum_{\substack{q^2/a \leq n \leq x \\ (an,q)=(h,q)}} f(n)\chi\left(\tfrac{an}{(h,q)}\right) + \mathcal{O}(x^{\delta+\varepsilon}).$$

We now split the remaining sum into two parts, denoted by $\tilde{M}_f^{(1)}(x; a, h)$ and $\tilde{M}_f^{(2)}(x; a, h)$, depending on whether $\operatorname{cond}(\chi) \mid D$ or not. A simple reordering of the sums shows that the first part is equal to

$M_f(x; a, h)$ as given in Theorem 1.2. The second part can be written as

$$M_f^{(2)}(x; a, h) = 2 \sum_{t \mid (a,h)} \sum_{\substack{u \mid h/t \\ (u,a/t)=1}} \sum_{q \le \sqrt{ax}/(tu)} \frac{1}{\varphi(q)} \sum_{\substack{\chi \bmod q \\ \text{cond}\,\chi \le R \\ \text{cond}(\chi) \nmid D}} \overline{\chi}\big(\tfrac{h}{tu}\big)\chi\big(\tfrac{a}{t}\big)\big(S_{f,\chi}(x, u) - S_{f,\chi}\big(\tfrac{tu^2q^2}{a}, u\big)\big),$$

with $S_{f,\chi}(x, u)$ given by

$$S_{f,\chi}(x, u) := \sum_{n \le x/u} f(un)\chi(n).$$

This last sum can be estimated via Lemma 8.1, namely we have

$$\begin{aligned} S_{f,\chi}(x, u) &= \sum_{\substack{u^* \mid u^\infty \\ u^* \le \sqrt{x}}} f(uu^*)\chi(u^*) \sum_{\substack{n \le x/(uu^*) \\ (n,u)=1}} f(n)\chi(n) + \mathcal{O}(x^{1/2+\varepsilon}) \\ &\ll x e^{-c\sqrt{\log x}} \sum_{u^* \le \sqrt{x}} \frac{\tau_A(uu^*)}{uu^*} + x^{1/2+\varepsilon} \\ &\ll \frac{\tau_A(u)}{u} x(\log x)^A e^{-c\sqrt{\log x}}, \end{aligned}$$

for some constant $c > 0$ depending on A, D and L. Hence

$$M_f^{(2)}(x; a, h) \ll \tau((a, h)) R x (\log x)^{A+2} e^{-c\sqrt{\log x}} \ll \tau((a, h)) x e^{-(c/2)\sqrt{\log x}}.$$

Eventually, we get

$$D_f(x; a, h) = M_f(x; a, h) + \mathcal{O}\bigg(\tau((a, h)) x \bigg(\frac{(\log x)^B}{R^{1/3}} + e^{-(c/2)\sqrt{\log x}}\bigg)\bigg),$$

and Theorem 1.2 follows with the choice $L = 3N + 3B$.

8A. *Proof of Theorems 1.3, 1.4 and 1.6.* The applications mentioned in the introduction are essentially all immediate corollaries of Theorem 1.2, except for the fact that it remains to evaluate the main terms. This is a rather tedious task, but can be done using standard techniques from analytic number theory, in particular the Selberg–Delange method, which is for example described in detail in [Tenenbaum 1995, Chapter II.5]. In order to not further lengthen this article, we only want to indicate very briefly the main steps of the procedure.

In the case of Theorem 1.3, the main term takes the form

$$M_{\tau_z}(x; 1, h) = 2 \sum_{q \le \sqrt{x}} \frac{1}{\varphi\big(\frac{q}{(h,q)}\big)} \sum_{\substack{q^2 \le n \le x \\ (n,q)=(h,q)}} \tau_z(n),$$

which after a few simple transformations can be written as

$$M_{\tau_z}(x;1,h)=\sum_{\substack{u\,|\,h,v\,|\,u^\infty\\ v\le\sqrt{x}}}\tau_z(uv)\sum_{\substack{q\le\sqrt{x}/u\\ (q,vh/u)=1}}\frac{D(x;uq,uv)-D(u^2q^2;uq,uv)}{\varphi(q)}+\mathcal{O}(x^{1/2+\varepsilon}),\tag{8-3}$$

where

$$D(y;r,t):=\sum_{\substack{n\le y/t\\ (n,r)=1}}\tau_z(n).$$

This sum has been studied in detail in [Tenenbaum 1995, Chapter II.5]. In particular, following the proof of [loc. cit., Theorem II.5.2], we see that there exist complex numbers $\mu_\ell^z(r,t)$ such that

$$D(y;r,t)=\frac{1}{2\pi i}\sum_{\ell=0}^{L}\frac{\mu_\ell^z(r,t)}{\Gamma(z-\ell)}\frac{y(\log y)^z}{(\log y)^{\ell+1}}+\mathcal{O}\biggl(\frac{(\log t)^{L+1}}{t}\frac{y(\log y)^z}{(\log y)^{L+2-\varepsilon}}\biggr),$$

where

$$\mu_\ell^z(r,t):=\Delta_s^\ell\biggl(\frac{\psi_s^z(r)}{t^s}\frac{(s-1)^z\zeta(s)^z}{s}\biggr)\quad\text{with }\psi_s^z(r):=\prod_{p\,|\,r}\Bigl(1-\frac{1}{p^s}\Bigr)^z,$$

and where the differential operator Δ_s^ℓ is defined as

$$\Delta_s^\ell:=\frac{1}{\ell!}\frac{\partial^\ell}{\partial s^\ell}\bigg|_{s=1}.$$

By Leibniz's rule and the Taylor expansion of $(s-1)\zeta(s)$ at 1, it remains to evaluate the sums

$$\sum_{\substack{q\le\sqrt{x}/u\\ (q,vh/u)=1}}\frac{\Delta_s^\ell\psi_s^z(uq)}{\varphi(q)}\quad\text{and}\quad\sum_{\substack{q\le\sqrt{x}/u\\ (q,vh/u)=1}}\frac{\Delta_s^\ell\psi_s^z(uq)}{\varphi(q)}\frac{q^2(2\log(uq))^z}{(2\log(uq))^{\ell-1}}.$$

For the first sum this is a standard exercise in using counter integration, the result being

$$\sum_{\substack{q\le\sqrt{x}/u\\ (q,vh/u)=1}}\frac{\Delta_s^\ell\psi_s^z(uq)}{\varphi(q)}=\Delta_s^\ell\operatorname*{Res}_{w=0}\biggl(C_{s,w}^z\frac{\psi_s^z(u)\rho_w\bigl(\frac{vh}{u}\bigr)}{\gamma_{s,w}^z(h)}\frac{x^{w/2}}{u^w}\frac{\zeta(w+1)}{w}\biggr)+\mathcal{O}\biggl(\frac{1}{x^{2/3-\varepsilon}}\biggr),$$

with

$$C_{s,w}^z:=\prod_p\biggl(1+\frac{1}{(p-1)p^{w+1}}+\frac{\psi_s^z(p)-1}{(p-1)p^w}\biggr),$$

and

$$\gamma_{s,w}^z(n):=\prod_{p\,|\,n}\biggl(1+\frac{p(\psi_s^z(p)-1)}{p^{w+2}-p^{w+1}+1}\biggr)\quad\text{and}\quad\rho_w(n):=\prod_{p\,|\,n}\biggl(1-\frac{p}{p^{w+2}-p^{w+1}+1}\biggr).$$

An asymptotic formula for the second sum now follows via partial summation. After putting the resulting formulae back in (8-3) and completing the sum over v, this eventually leads to the main term described in

Theorem 1.3. In particular, the first coefficient is given by

$$\lambda_{h,0}(z)=\frac{1}{\Gamma(z)}\prod_{(p,h)=1}\left(1+\frac{(1-1/p)^{z-1}-1}{p}\right)\cdot\prod_{p^\ell\|h}\left(1-\frac{1}{p}+\left(1-\frac{1}{p}\right)^{z+1}\sum_{j=1}^{\ell-1}\frac{(\ell-j)\tau_z(p^j)}{p^j}+\left(1-\frac{1}{p}\right)^{z-1}\frac{\tau_z(p^\ell)}{p^{\ell+1}}\right). \tag{8-4}$$

For Corollary 1.5, we have from [Narkiewicz 2004, Proposition 8.4, Theorem 8.6] that the characteristic function $n\mapsto b_K(n)$ of the set $\mathcal{N}_K$ is multiplicative with $b(p)=1$ if and only if $\sum_{\chi\in X(K)}\chi(p)>0$, where $X(K)$ is a subgroup of the Dirichlet characters modulo the discriminant $D=\operatorname{Disc}(K)$ and $p\nmid D$. The subgroup of residue classes $a \bmod D$ such that $\sum_{\chi\in X(K)}\chi(a)>0$, corresponding to the subgroup H in [Narkiewicz 2004, Theorem 8.2], has density $1/[K:\mathbb{Q}]$ inside $(\mathbb{Z}/D\mathbb{Z})^\times$. Thus we have a factorization

$$\sum_{n\geq 1}\frac{b_K(n)}{n^s}=\zeta(s)^{1/[K:\mathbb{Q}]}H(s)$$

where H is holomorphic and bounded in the strip $\mathfrak{Re}(s)\geq\frac{2}{3}$. The rest of the argument the follows the path described above. We leave the details to the reader.

In the case $K=\mathbb{Q}(i)$, the first coefficient is given by $\beta_{h,0}=B_0B(h)$, where

$$B_0:=\frac{1}{\sqrt{2}}\prod_{p\equiv 3 \bmod 4}\left(1-\frac{1}{p^2}\right)^{-1/2}, \tag{8-5}$$

and

$$B(h):=\left(1+\frac{\chi_4(h^*)}{4h^\circ}\right)\prod_{\substack{p^\ell\,\|\,h\\ p\equiv 3 \bmod 4}}\left(1-\frac{1}{p+1}+\frac{(-1)^\ell}{p^\ell(p+1)}\right)\prod_{p\equiv 3 \bmod 4}\left(1+\frac{1}{p^2}\right),$$

with $h^\circ:=(h,2^\infty)$, $h^*:=\frac{h}{h^\circ}$ and χ_4 the nonprincipal character mod 4.

Finally, the proof of Theorem 1.6 rests upon the fact that

$$\sum_{\substack{|h|<n\leq x\\ \omega(n)=k}}\tau(n-h)=\frac{1}{k!}\frac{\partial^k}{\partial z^k}\Xi_{x,h}(0)\quad\text{with } \Xi_{x,h}(z):=\sum_{|h|<n\leq x}z^{\omega(n)}\tau(n-h).$$

Since the function $n\mapsto z^{\omega(n)}$ is an element of $\mathcal{F}_1(A)$ for $|z|\leq A$, Theorem 1.2 can again be applied in this case. After evaluating the arising main term in the same manner as described above, we see that there exist functions $\gamma_{h,\ell}(z)$, which are holomorphic in a neighborhood of z, such that

$$\Xi_{x,h}(z)=x(\log x)^z\sum_{\ell=0}^{L}\frac{\gamma_{h,\ell}(z)}{(\log x)^\ell}+\mathcal{O}\left(\frac{x(\log x)^{\mathfrak{Re}(z)}}{(\log x)^{L+1-\varepsilon}}\right).$$

At this point Theorem 1.6 essentially follows by taking derivatives with respect to z on both sides. The procedure is however not completely straightforward, since we also need to have control over the error term on the right hand side. In our case we can simply cite [Tenenbaum 1995, Theorem II.6.3], where a result of this type is proven in very large generality.

References

[Andrade et al. 2015] J. C. Andrade, L. Bary-Soroker, and Z. Rudnick, "Shifted convolution and the Titchmarsh divisor problem over $\mathbb{F}_q[t]$", *Philos. Trans. Roy. Soc. A* **373**:2040 (2015), art. id. 20140308. Correction in *Philos. Trans. Roy. Soc. A* **373**:2060 (2015), art. id. 20140308. MR Zbl

[Barban and Vehov 1969] M. B. Barban and P. P. Vehov, "Summation of multiplicative functions of polynomials", *Mat. Zametki* **5** (1969), 669–680. In Russian; translated in *Math. Notes* **5**:6 (1969), 400–407. MR Zbl

[Bary-Soroker and Fehm 2019] L. Bary-Soroker and A. Fehm, "Correlations of sums of two squares and other arithmetic functions in function fields", *Int. Math. Res. Not.* **2019**:14 (2019), 4469–4515. MR

[Bombieri 1965] E. Bombieri, "On the large sieve", *Mathematika* **12** (1965), 201–225. MR Zbl

[Bombieri et al. 1986] E. Bombieri, J. B. Friedlander, and H. Iwaniec, "Primes in arithmetic progressions to large moduli", *Acta Math.* **156**:3-4 (1986), 203–251. MR Zbl

[Conrey and Keating 2016] B. Conrey and J. P. Keating, "Moments of zeta and correlations of divisor-sums, IV", *Res. Number Theory* **2** (2016), art. id. 24. MR Zbl

[Deshouillers and Iwaniec 1982a] J.-M. Deshouillers and H. Iwaniec, "An additive divisor problem", *J. Lond. Math. Soc.* (2) **26**:1 (1982), 1–14. MR Zbl

[Deshouillers and Iwaniec 1982b] J.-M. Deshouillers and H. Iwaniec, "Kloosterman sums and Fourier coefficients of cusp forms", *Invent. Math.* **70**:2 (1982), 219–288. MR Zbl

[Drappeau 2015] S. Drappeau, "Théorèmes de type Fouvry–Iwaniec pour les entiers friables", *Compos. Math.* **151**:5 (2015), 828–862. MR Zbl

[Drappeau 2017] S. Drappeau, "Sums of Kloosterman sums in arithmetic progressions, and the error term in the dispersion method", *Proc. Lond. Math. Soc.* (3) **114**:4 (2017), 684–732. MR Zbl

[Elliott 1994] P. D. T. A. Elliott, *On the correlation of multiplicative and the sum of additive arithmetic functions*, Mem. Amer. Math. Soc. **538**, Amer. Math. Soc., Providence, RI, 1994. MR Zbl

[Fouvry 1981] É. Fouvry, *Répartition des suites dans les progressions arithmétiques: résultats du type Bombieri–Vinogradov avec exposant supérieur à* 1/2, Ph.D. thesis, Université de Bordeaux-I, 1981.

[Fouvry 1984] É. Fouvry, "Autour du théorème de Bombieri–Vinogradov", *Acta Math.* **152**:3-4 (1984), 219–244. MR Zbl

[Fouvry 1985] É. Fouvry, "Sur le problème des diviseurs de Titchmarsh", *J. Reine Angew. Math.* **357** (1985), 51–76. MR Zbl

[Fouvry and Iwaniec 1983] É. Fouvry and H. Iwaniec, "Primes in arithmetic progressions", *Acta Arith.* **42**:2 (1983), 197–218. MR Zbl

[Fouvry and Radziwiłł 2018] É. Fouvry and Radziwiłł, "Level of distribution of unbalanced convolutions", preprint, 2018. arXiv

[Fouvry and Tenenbaum 1985] É. Fouvry and G. Tenenbaum, "Sur la corrélation des fonctions de Piltz", *Rev. Mat. Iberoam.* **1**:3 (1985), 43–54. MR Zbl

[Fouvry and Tenenbaum 1990] É. Fouvry and G. Tenenbaum, "Diviseurs de Titchmarsh des entiers sans grand facteur premier", pp. 86–102 in *Analytic number theory* (Tokyo, 1988), edited by K. Nagasaka and E. Fouvry, Lecture Notes in Math. **1434**, Springer, 1990. MR Zbl

[Fouvry and Tenenbaum 1996] É. Fouvry and G. Tenenbaum, "Répartition statistique des entiers sans grand facteur premier dans les progressions arithmétiques", *Proc. Lond. Math. Soc.* (3) **72**:3 (1996), 481–514. MR Zbl

[Freiberg et al. 2017] T. Freiberg, P. Kurlberg, and L. Rosenzweig, "Poisson distribution for gaps between sums of two squares and level spacings for toral point scatterers", *Commun. Number Theory Phys.* **11**:4 (2017), 837–877. MR Zbl

[Friedlander and Iwaniec 1985] J. B. Friedlander and H. Iwaniec, "Incomplete Kloosterman sums and a divisor problem", *Ann. of Math.* (2) **121**:2 (1985), 319–350. MR Zbl

[Gallagher 1968] P. X. Gallagher, "Bombieri's mean value theorem", *Mathematika* **15** (1968), 1–6. MR Zbl

[Granville and Shao 2018] A. Granville and X. Shao, "When does the Bombieri–Vinogradov theorem hold for a given multiplicative function?", *Forum Math. Sigma* **6** (2018), art. id. e15. MR Zbl

[Green 2018] B. Green, "A note on multiplicative functions on progressions to large moduli", *Proc. Roy. Soc. Edinburgh Sect. A* **148**:1 (2018), 63–77. MR Zbl

[Halberstam 1967] H. Halberstam, "Footnote to the Titchmarsh–Linnik divisor problem", *Proc. Amer. Math. Soc.* **18** (1967), 187–188. MR Zbl

[Harper 2012] A. J. Harper, "Bombieri–Vinogradov and Barban–Davenport–Halberstam type theorems for smooth numbers", preprint, 2012. arXiv

[Heath-Brown 1982] D. R. Heath-Brown, "Prime numbers in short intervals and a generalized Vaughan identity", *Canad. J. Math.* **34**:6 (1982), 1365–1377. MR Zbl

[Henriot 2012] K. Henriot, "Nair–Tenenbaum bounds uniform with respect to the discriminant", *Math. Proc. Cambridge Philos. Soc.* **152**:3 (2012), 405–424. Correction in **157**:2 (2014), 375–377. MR Zbl

[Hmyrova 1964] N. A. Hmyrova, "On polynomials with small prime divisors", *Dokl. Akad. Nauk SSSR* **155** (1964), 1268–1271. In Russian; translated in *Soviet Math. Dokl.* **5** (1964), 576–579. MR Zbl

[Ivić 1991] A. Ivić, *Lectures on mean values of the Riemann zeta function*, Tata Inst. Fund. Res. Lect. Math. Phys. **82**, Springer, 1991. MR Zbl

[Iwaniec 1976] H. Iwaniec, "The half dimensional sieve", *Acta Arith.* **29**:1 (1976), 69–95. MR Zbl

[Iwaniec 2002] H. Iwaniec, *Spectral methods of automorphic forms*, 2nd ed., Graduate Studies in Mathematics **53**, Amer. Math. Soc., Providence, RI, 2002. MR Zbl

[Iwaniec and Kowalski 2004] H. Iwaniec and E. Kowalski, *Analytic number theory*, Amer. Math. Soc. Colloq. Publ. **53**, Amer. Math. Soc., Providence, RI, 2004. MR Zbl

[Khripunova 1998] M. B. Khripunova, "Additive problems with numbers that have a given number of prime divisors", *Mat. Zametki* **63**:5 (1998), 749–762. In Russian; translated in *Math. Notes* **63**:5 (1998), 658–669. MR Zbl

[Linnik 1963] J. V. Linnik, *The dispersion method in binary additive problems*, Amer. Math. Soc., Providence, RI, 1963. MR Zbl

[Matomäki et al. 2019a] K. Matomäki, M. Radziwiłł, and T. Tao, "Correlations of the von Mangoldt and higher divisor functions, I: Long shift ranges", *Proc. Lond. Math. Soc.* (3) **118**:2 (2019), 284–350. MR Zbl

[Matomäki et al. 2019b] K. Matomäki, M. Radziwiłł, and T. Tao, "Correlations of the von Mangoldt and higher divisor functions, II: Divisor correlations in short ranges", *Math. Ann.* **374**:1-2 (2019), 793–840. MR Zbl

[Matthiesen 2012] L. Matthiesen, "Correlations of the divisor function", *Proc. Lond. Math. Soc.* (3) **104**:4 (2012), 827–858. MR Zbl

[Matthiesen 2016] L. Matthiesen, "Linear correlations of multiplicative functions", preprint, 2016. To appear in *Proc. Lond. Math. Soc.* arXiv

[Meurman 2001] T. Meurman, "On the binary additive divisor problem", pp. 223–246 in *Number theory* (Turku, Finland, 1999), edited by M. Jutila and T. Metsänkylä, de Gruyter, Berlin, 2001. MR Zbl

[Michel 2007] P. Michel, "Analytic number theory and families of automorphic L-functions", pp. 181–295 in *Automorphic forms and applications* (Park City, UT, 2002), edited by P. Sarnak and F. Shahidi, IAS/Park City Math. Ser. **12**, Amer. Math. Soc., Providence, RI, 2007. MR Zbl

[Mikawa 1992] H. Mikawa, "On prime twins in arithmetic progressions", *Tsukuba J. Math.* **16**:2 (1992), 377–387. MR Zbl

[Montgomery and Vaughan 2007] H. L. Montgomery and R. C. Vaughan, *Multiplicative number theory, I: Classical theory*, Cambridge Stud. Adv. Math. **97**, Cambridge Univ. Press, 2007. MR Zbl

[Motohashi 1980] Y. Motohashi, "An asymptotic series for an additive divisor problem", *Math. Z.* **170**:1 (1980), 43–63. MR Zbl

[Motohashi 1994] Y. Motohashi, "The binary additive divisor problem", *Ann. Sci. École Norm. Sup.* (4) **27**:5 (1994), 529–572. MR Zbl

[Narkiewicz 2004] W. Narkiewicz, *Elementary and analytic theory of algebraic numbers*, 3rd ed., Springer, 2004. MR Zbl

[Ng and Thom 2019] N. Ng and M. Thom, "Bounds and conjectures for additive divisor sums", *Funct. Approx. Comment. Math.* **60**:1 (2019), 97–142. MR Zbl

[Pitt 2013] N. J. E. Pitt, "On an analogue of Titchmarsh's divisor problem for holomorphic cusp forms", *J. Amer. Math. Soc.* **26**:3 (2013), 735–776. MR Zbl

[Ramaré 2013] O. Ramaré, "Prime numbers: emergence and victories of bilinear forms decomposition", *Eur. Math. Soc. Newsl.* **90** (2013), 18–27. MR Zbl

[Rodriquez 1965] G. Rodriquez, "Sul problema dei divisori di Titchmarsh", *Boll. Un. Mat. Ital.* (3) **20** (1965), 358–366. MR Zbl

[Selberg 1954] A. Selberg, "Note on a paper by L. G. Sathe", *J. Indian Math. Soc.* (*N.S.*) **18**:1 (1954), 83–87. MR Zbl

[Selberg 1991] A. Selberg, *Collected papers, II*, Springer, 1991. MR Zbl

[Shiu 1980] P. Shiu, "A Brun–Titchmarsh theorem for multiplicative functions", *J. Reine Angew. Math.* **313** (1980), 161–170. MR Zbl

[Tao 2016] T. Tao, "The logarithmically averaged Chowla and Elliott conjectures for two-point correlations", *Forum Math. Pi* **4** (2016), art. id. e8. MR Zbl

[Tao and Teräväinen 2019] T. Tao and J. Teräväinen, "The structure of logarithmically averaged correlations of multiplicative functions, with applications to the Chowla and Elliott conjectures", *Duke Math. J.* **168**:11 (2019), 1977–2027. MR

[Tenenbaum 1995] G. Tenenbaum, *Introduction to analytic and probabilistic number theory*, 2nd ed., Cambridge Stud. Adv. Math. **46**, Cambridge Univ. Press, 1995. MR Zbl

[Titchmarsh 1930] E. C. Titchmarsh, "A divisor problem", *Rend. Circ. Mat. Palermo* **54**:1 (1930), 414–429. Correction in **57**:1 (1933), 478–479. Zbl

[Topacogullari 2016] B. Topacogullari, "The shifted convolution of divisor functions", *Q. J. Math.* **67**:2 (2016), 331–363. MR Zbl

[Topacogullari 2017] B. Topacogullari, "On a certain additive divisor problem", *Acta Arith.* **181**:2 (2017), 143–172. MR Zbl

[Topacogullari 2018] B. Topacogullari, "The shifted convolution of generalized divisor functions", *Int. Math. Res. Not.* **2018**:24 (2018), 7681–7724. MR Zbl

[Vaughan 1975] R. C. Vaughan, "Mean value theorems in prime number theory", *J. Lond. Math Soc.* (2) **10** (1975), 153–162. MR Zbl

[Vaughan 1989] R. C. Vaughan, "A new iterative method in Waring's problem", *Acta Math.* **162**:1-2 (1989), 1–71. MR Zbl

[Vinogradov 1937] I. M. Vinogradov, "Representation of an odd number as a sum of three primes", *Dokl. Akad. Nauk SSSR* **15** (1937), 291–294. In Russian; translated in Vinogradov, *Selected Works*, Springer (1985), pp. 129–132.

[Vinogradov 1965] A. I. Vinogradov, "The density hypothesis for Dirichet L-series", *Izv. Akad. Nauk SSSR Ser. Mat.* **29** (1965), 903–934. In Russian; translated in *Amer. Math. Soc. Transl. (2)* **82** (1969) 9–46. Correction (in Russian) in **30**:3 (1966), 719–720. MR

Communicated by Roger Heath-Brown
Received 2018-12-17 Revised 2019-07-01 Accepted 2019-07-31

sary-aurelien.drappeau@univ-amu.fr *Institut de Mathématiques de Marseille, Aix-Marseille Université, CNRS, Centrale Marseille, Faculté des sciences de Luminy, Marseille, France*

berke.topacogullari@epfl.ch *EPFL SB MATH TAN, Station 8, 1015 Lausanne, Switzerland*

ALGEBRA AND NUMBER THEORY 13:10 (2019)
dx.doi.org/10.2140/ant.2019.13.2427

The construction problem for Hodge numbers modulo an integer

Matthias Paulsen and Stefan Schreieder

For any integer $m \geq 2$ and any dimension $n \geq 1$, we show that any n-dimensional Hodge diamond with values in $\mathbb{Z}/m\mathbb{Z}$ is attained by the Hodge numbers of an n-dimensional smooth complex projective variety. As a corollary, there are no polynomial relations among the Hodge numbers of n-dimensional smooth complex projective varieties besides the ones induced by the Hodge symmetries, which answers a question raised by Kollár in 2012.

1. Introduction

Hodge theory allows one to decompose the k-th Betti cohomology of an n-dimensional compact Kähler manifold X into its (p, q)-pieces for all $0 \leq k \leq 2n$:

$$H^k(X, \mathbb{C}) = \bigoplus_{\substack{p+q=k \\ 0 \leq p,q \leq n}} H^{p,q}(X), \qquad \overline{H^{p,q}(X)} = H^{q,p}(X).$$

The $\mathbb{C}$-linear subspaces $H^{p,q}(X)$ are naturally isomorphic to the Dolbeault cohomology groups $H^q(X, \Omega^p_X)$.

The integers $h^{p,q}(X) = \dim_{\mathbb{C}} H^{p,q}(X)$ for $0 \leq p, q \leq n$ are called Hodge numbers. One usually arranges them in the so called Hodge diamond:

$$\begin{array}{ccccccccc}
 & & & & h^{n,n} & & & & \\
 & & & h^{n,n-1} & & h^{n-1,n} & & & \\
 & & \iddots & & \vdots & & \ddots & & \\
 & h^{n,1} & & & & & & h^{1,n} & \\
h^{n,0} & & h^{n-1,1} & & \cdots & & h^{1,n-1} & & h^{0,n} \\
 & h^{n-1,0} & & & & & & h^{0,n-1} & \\
 & & \ddots & & \vdots & & \iddots & & \\
 & & & h^{1,0} & & h^{0,1} & & & \\
 & & & & h^{0,0} & & & &
\end{array}$$

The sum of the k-th row of the Hodge diamond equals the k-th Betti number. We always assume that a Kähler manifold is compact and connected, so we have $h^{0,0} = h^{n,n} = 1$.

MSC2010: primary 32Q15; secondary 14C30, 14E99, 51M15.
Keywords: Hodge numbers, Kähler manifolds, construction problem.

Complex conjugation and Serre duality induce the symmetries

$$h^{p,q} = h^{q,p} = h^{n-p,n-q} \quad \text{for all } 0 \le p, q \le n. \tag{1}$$

Additionally, we have the Lefschetz inequalities

$$h^{p,q} \le h^{p+1,q+1} \quad \text{for } p+q < n. \tag{2}$$

While Hodge theory places severe restrictions on the geometry and topology of Kähler manifolds, Simpson [2004] points out that very little is known to which extent the theoretically possible phenomena actually occur. This leads to the following construction problem for Hodge numbers:

Question 1. Let $(h^{p,q})_{0 \le p,q \le n}$ be a collection of nonnegative integers with $h^{0,0} = 1$ obeying the Hodge symmetries (1) and the Lefschetz inequalities (2). Does there exist a Kähler manifold X such that $h^{p,q}(X) = h^{p,q}$ for all $0 \le p, q \le n$?

After results in dimensions two and three (see e.g., [Hunt 1989]), significant progress has been made by Schreieder [2015]. For instance, it is shown in [loc. cit., Theorem 3] that the above construction problem is fully solvable for large parts of the Hodge diamond in arbitrary dimensions. In particular, the Hodge numbers in a given weight k may be arbitrary (up to a quadratic lower bound on $h^{p,p}$ if $k = 2p$ is even) and so the outer Hodge numbers can be far larger than the inner Hodge numbers (see [loc. cit., Theorem 1]), contradicting earlier expectations formulated in [Simpson 2004]. Weaker results with simpler proofs, concerning the possible Hodge numbers in a given weight, have later been obtained by Arapura [2016].

In [Schreieder 2015], it was also observed that one cannot expect a positive answer to Question 1 in its entirety. For example, any 3-dimensional Kähler manifold X with $h^{1,1}(X) = 1$ and $h^{2,0}(X) \ge 1$ satisfies $h^{2,1}(X) < 12^6 \cdot h^{3,0}(X)$, see [loc. cit., Proposition 28]. Therefore, a complete classification of all possible Hodge diamonds of Kähler manifolds or smooth complex projective varieties seems hopelessly complicated.

While these inequalities aggravate the construction problem for Hodge numbers, one might ask whether there also exist number theoretic obstructions for possible Hodge diamonds. For example, the Chern numbers of Kähler manifolds satisfy certain congruences due to integrality conditions implied by the Hirzebruch–Riemann–Roch theorem.

For an arbitrary integer $m \ge 2$, let us consider the Hodge numbers of a Kähler manifold in $\mathbb{Z}/m\mathbb{Z}$, which forces all inequalities to disappear. The purpose of this paper is to show that Question 1 is modulo m completely solvable even for smooth complex projective varieties.

Theorem 2. *Let $m \ge 2$ be an integer. For any integer $n \ge 1$ and any collection of integers $(h^{p,q})_{0 \le p,q \le n}$ such that $h^{0,0} = 1$ and $h^{p,q} = h^{q,p} = h^{n-p,n-q}$ for $0 \le p, q \le n$, there exists a smooth complex projective variety X of dimension n such that*

$$h^{p,q}(X) \equiv h^{p,q} \pmod{m}$$

for all $0 \le p, q \le n$.

Therefore, the Hodge numbers of Kähler manifolds do not follow any number theoretic rules, and the behavior of smooth complex projective varieties is the same in this aspect.

As a consequence of Theorem 2, we show:

Corollary 3. *Up to the Hodge symmetries (1), there are no polynomial relations among the Hodge numbers of smooth complex projective varieties of the same dimension.*

In particular, there are no polynomial relations in the strictly larger class of Kähler manifolds, which was a question raised by Kollár after a colloquium talk of Kotschick at the University of Utah in fall 2012. For linear relations among Hodge numbers, this question was settled in work of Kotschick and Schreieder [2013].

We call the Hodge numbers $h^{p,q}(X)$ with $p \in \{0, n\}$ or $q \in \{0, n\}$ (i.e., the ones placed on the border of the Hodge diamond) the *outer Hodge numbers* of X and the remaining ones the *inner Hodge numbers*. Note that the outer Hodge numbers are birational invariants and are thus determined by the birational equivalence class of X.

Our proof shows (see Theorem 5 below) that any smooth complex projective variety is birational to a smooth complex projective variety with prescribed inner Hodge numbers in $\mathbb{Z}/m\mathbb{Z}$. As a corollary, there are no polynomial relations among the inner Hodge numbers within a given birational equivalence class. This is again a generalization of the corresponding result for linear relations obtained in [Kotschick and Schreieder 2013, Theorem 2].

The proof of Theorem 2 can thus be divided into two steps: First we solve the construction problem modulo m for the outer Hodge numbers. This is done in Section 2. Then we show the aforementioned result that the inner Hodge numbers can be adjusted arbitrarily in $\mathbb{Z}/m\mathbb{Z}$ via birational equivalences (in fact, via repeated blow-ups). This is done in Section 3. Finally, in Section 4 we deduce that no nontrivial polynomial relations between Hodge numbers exist, thus answering Kollár's question.

2. Outer Hodge numbers

We prove the following statement via induction on the dimension $n \geq 1$.

Proposition 4. *For any collection of integers $(h^{p,0})_{1\leq p\leq n}$, there exists a smooth complex projective variety X_n of dimension n together with a very ample line bundle L_n on X_n such that*

$$h^{p,0}(X_n) \equiv h^{p,0} \pmod{m}$$

for all $1 \leq p \leq n$ and

$$\chi(L_n^{-1}) \equiv 1 \pmod{m}.$$

Proof. We take X_1 to be a curve of genus g where $g \equiv h^{1,0} \pmod{m}$. Further, we take L_1 to be a line bundle of degree d on X_1 where $d > 2g$ and $d \equiv -g \pmod{m}$. Then L_1 is very ample and by the Riemann–Roch theorem we have $\chi(L_1^{-1}) \equiv 1 \pmod{m}$.

Now let $n > 1$. We define a collection of integers $(k^{p,0})_{-1\le p\le n-1}$ recursively via

$$k^{-1,0} = 0, \quad k^{0,0} = 1, \quad k^{p,0} = h^{p,0} - 2k^{p-1,0} - k^{p-2,0} \text{ for } 1 \le p \le n-1.$$

We choose X_{n-1} and L_{n-1} by induction hypothesis such that $h^{p,0}(X_{n-1}) \equiv k^{p,0} \pmod m$ for all $1 \le p \le n-1$.

Let E be a smooth elliptic curve and let L be a very ample line bundle of degree d on E such that $d \equiv 1 \pmod m$. Let e be a positive integer such that

$$e \equiv 1 + \sum_{p=1}^{n} (-1)^p h^{p,0} \pmod m.$$

Let $X_n \subset X_{n-1} \times E \times E$ be a hypersurface defined by a general section of the very ample line bundle

$$P_n = \mathrm{pr}_1^* L_{n-1} \otimes \mathrm{pr}_2^* L^{m-1} \otimes \mathrm{pr}_3^* L^e$$

on $X_{n-1} \times E \times E$. By Bertini's theorem, we may assume X_n to be smooth and irreducible. Let L_n be the restriction to X_n of the very ample line bundle

$$Q_n = \mathrm{pr}_1^* L_{n-1} \otimes \mathrm{pr}_2^* L \otimes \mathrm{pr}_3^* L$$

on $X_{n-1} \times E \times E$. Then L_n is again very ample.

By the Lefschetz hyperplane theorem, we have

$$h^{p,0}(X_n) = h^{p,0}(X_{n-1} \times E \times E)$$

for all $1 \le p \le n-1$. Since the Hodge diamond of $E \times E$ is

$$\begin{array}{ccccc} & & 1 & & \\ & 2 & & 2 & \\ 1 & & 4 & & 1, \\ & 2 & & 2 & \\ & & 1 & & \end{array}$$

Künneth's formula yields

$$h^{p,0}(X_n) = h^{p,0}(X_{n-1}) + 2h^{p-1,0}(X_{n-1}) + h^{p-2,0}(X_{n-1}) \equiv k^{p,0} + 2k^{p-1,0} + k^{p-2,0} = h^{p,0} \pmod m$$

for all $1 \le p \le n-1$. Therefore, it only remains to show that $h^{n,0}(X_n) \equiv h^{n,0} \pmod m$ and $\chi(L_n^{-1}) \equiv 1 \pmod m$. Since

$$\chi(\mathcal{O}_{X_n}) = 1 + \sum_{p=1}^{n} (-1)^p h^{p,0}(X_n),$$

the congruence $h^{n,0}(X_n) \equiv h^{n,0} \pmod m$ is equivalent to $\chi(\mathcal{O}_{X_n}) \equiv e \pmod m$.

By definition of X_n, the ideal sheaf on $X_{n-1}\times E\times E$ of regular functions vanishing on X_n is isomorphic to the sheaf of sections of the dual line bundle P_n^{-1}. Hence, there is a short exact sequence

$$0\to P_n^{-1}\to \mathcal{O}_{X_{n-1}\times E\times E}\to i_*\mathcal{O}_{X_n}\to 0 \tag{3}$$

of sheaves on $X_{n-1}\times E\times E$ where $i\colon X_n\to X_{n-1}\times E\times E$ denotes the inclusion. Together with Künneth's formula and the Riemann–Roch theorem, we obtain

$$\chi(\mathcal{O}_{X_n})=\chi(\mathcal{O}_{X_{n-1}\times E\times E})-\chi(P_n^{-1})=\chi(\mathcal{O}_{X_{n-1}})\underbrace{\chi(\mathcal{O}_E)^2}_{=0}-\underbrace{\chi(L_{n-1}^{-1})}_{\equiv 1}\underbrace{\chi(L^{1-m})}_{\equiv 1}\underbrace{\chi(L^{-e})}_{\equiv -e}\equiv e \pmod m.$$

Tensoring (3) with Q_n^{-1} yields the short exact sequence

$$0\to P_n^{-1}\otimes Q_n^{-1}\to Q_n^{-1}\to i_*i^*Q_n^{-1}\to 0$$

and thus

$$\chi(L_n^{-1})=\chi(Q_n^{-1})-\chi(P_n^{-1}\otimes Q_n^{-1})=\underbrace{\chi(L_{n-1}^{-1})}_{\equiv 1}\underbrace{\chi(L^{-1})^2}_{\equiv 1}-\chi(L_{n-1}^{-2})\underbrace{\chi(L^{-m})}_{\equiv 0}\chi(L^{-e-1})\equiv 1 \pmod m.$$

This finishes the induction step. □

3. Inner Hodge numbers

We now show the following result, which significantly improves [Kotschick and Schreieder 2013, Theorem 2].

Theorem 5. *Let X be a smooth complex projective variety of dimension n and let $(h^{p,q})_{1\le p,q\le n-1}$ be any collection of integers such that $h^{p,q}=h^{q,p}=h^{n-p,n-q}$ for $1\le p,q\le n-1$. Then X is birational to a smooth complex projective variety X' such that*

$$h^{p,q}(X')\equiv h^{p,q} \pmod m$$

for all $1\le p,q\le n-1$.

Together with Proposition 4, this will complete the proof of Theorem 2.

Let us recall the following result on blow-ups, see e.g., [Voisin 2002, Theorem 7.31]: If $\tilde{X}$ denotes the blow-up of a Kähler manifold X along a closed submanifold $Z\subset X$ of codimension c, we have

$$H^{p,q}(\tilde{X})\cong H^{p,q}(X)\oplus\bigoplus_{i=1}^{c-1}H^{p-i,q-i}(Z).$$

Therefore,

$$h^{p,q}(\tilde{X})=h^{p,q}(X)+\sum_{i=1}^{c-1}h^{p-i,q-i}(Z). \tag{4}$$

In order to prove Theorem 5, we first show that we may assume that X contains certain subvarieties, without modifying its Hodge numbers modulo m.

Lemma 6. *Let X be a smooth complex projective variety of dimension n. Let $r, s \geq 0$ be integers such that $r+s \leq n-1$. Then X is birational to a smooth complex projective variety X' of dimension n such that $h^{p,q}(X') \equiv h^{p,q}(X) \pmod{m}$ for all $0 \leq p, q \leq n$ and such that X' contains at least m disjoint smooth closed subvarieties that are all isomorphic to a projective bundle of rank r over $\mathbb{P}^s$.*

Proof. We first blow up X in a point and denote the result by $\tilde{X}$. The exceptional divisor is a subvariety in $\tilde{X}$ isomorphic to $\mathbb{P}^{n-1}$. In particular, $\tilde{X}$ contains a copy of $\mathbb{P}^s \subset \mathbb{P}^{n-1}$. Now we blow up $\tilde{X}$ along $\mathbb{P}^s$ to obtain $\hat{X}$. The exceptional divisor in $\hat{X}$ is the projectivization of the normal bundle of $\mathbb{P}^s$ in $\tilde{X}$. Since $\mathbb{P}^s$ is contained in a smooth closed subvariety of dimension $r+s+1$ in $\tilde{X}$ (choose either $\mathbb{P}^{r+s+1} \subset \mathbb{P}^{n-1}$ if $r+s<n-1$ or $\tilde{X}$ if $r+s=n-1$), the normal bundle of $\mathbb{P}^s$ in $\tilde{X}$ contains a vector subbundle of rank $r+1$, and hence its projectivization contains a projective subbundle of rank r. Therefore, $\hat{X}$ admits a subvariety isomorphic to the total space of a projective bundle of rank r over $\mathbb{P}^s$.

By (4), the above construction only has an additive effect on the Hodge diamond, i.e., the differences between respective Hodge numbers of $\hat{X}$ and X are constants independent of X. Hence, we may apply the above construction $m-1$ more times to obtain a smooth complex projective variety X' containing m disjoint copies of the desired projective bundle and satisfying $h^{p,q}(X') \equiv h^{p,q}(X) \pmod{m}$. ☐

In the following, we consider the primitive Hodge numbers

$$l^{p,q}(X) = h^{p,q}(X) - h^{p-1,q-1}(X)$$

for $p+q \leq n$. Clearly, it suffices to show Theorem 5 for a given collection $(l^{p,q})_{(p,q)\in I}$ of primitive Hodge numbers instead, where

$$I = \{(p,q) \mid 1 \leq p \leq q \leq n-1 \text{ and } p+q \leq n\}.$$

This is because one can get back the original Hodge numbers from the primitive Hodge numbers via the relation

$$h^{p,q}(X) = h^{0,q-p}(X) + \sum_{i=1}^{p} l^{i,q-p+i}(X)$$

for $p \leq q$ and $p+q \leq n$, and $h^{0,q-p}(X)$ is a birational invariant.

We define a total order $\prec$ on I via

$$(r,s) \prec (p,q) \iff r+s < p+q \text{ or } (r+s = p+q \text{ and } s < q).$$

Proposition 7. *Let X be a smooth complex projective variety of dimension n. Let $(r,s) \in I$. Then X is birational to a smooth complex projective variety X' of dimension n such that*

$$l^{r,s}(X') \equiv l^{r,s}(X) + 1 \pmod{m} \quad \text{and} \quad l^{p,q}(X') \equiv l^{p,q}(X) \pmod{m}$$

for all $(p,q) \in I$ with $(r,s) \prec (p,q)$.

Proof. By Lemma 6, we may assume that X contains m disjoint copies of a projective bundle of rank $r-1$ over $\mathbb{P}^{s-r+1}$. Therefore, it is possible to blow up X along a projective bundle B_d of rank $r-1$ over smooth hypersurfaces $Y_d \subset \mathbb{P}^{s-r+1}$ of degree d (in case of $r = s$, Y_d just consists of d distinct points in $\mathbb{P}^1$) and we may repeat this procedure m times and with different values for d. The Hodge numbers of B_d are the same as for the trivial bundle $Y_d \times \mathbb{P}^{r-1}$, see e.g., [Voisin 2002, Lemma 7.32].

By the Lefschetz hyperplane theorem, the Hodge diamond of Y_d is the sum of the Hodge diamond of $Y_1 \cong \mathbb{P}^{s-r}$, having nonzero entries only in the middle column, and of a Hodge diamond depending on d, having nonzero entries only in the middle row. It is well known (e.g., by computing Euler characteristics as in Section 2) that the two outer entries of this middle row are precisely $\binom{d-1}{s-r+1}$.

Now we blow up X once along B_{s-r+2} and $m-1$ times along B_1 and denote the resulting smooth complex projective variety by X'. Due to (4) and Künneth's formula, this construction affects the Hodge numbers modulo m in the same way as if we would blow up a single subvariety $Z \times \mathbb{P}^{r-1} \subset X$, where Z is a (formal) $(s-r)$-dimensional Kähler manifold whose Hodge diamond is concentrated in the middle row and has outer entries equal to $\binom{s-r+2-1}{s-r+1} = 1$. In particular, we have $h^{p,q}(Z \times \mathbb{P}^{r-1}) = 0$ unless $s-r \le p+q \le s+r-2$ (and $p+q$ has the same parity as $s-r$) and $|p-q| \le s-r$. On the other hand, $h^{p,q}(Z \times \mathbb{P}^{r-1}) = 1$ if $s-r \le p+q \le s+r-2$ and $|p-q| = s-r$.

Taking differences in (4), it follows that

$$l^{p,q}(X') \equiv l^{p,q}(X) + h^{p-1,q-1}(Z \times \mathbb{P}^{r-1}) - h^{p-n+s-1,q-n+s-1}(Z \times \mathbb{P}^{r-1}) \pmod m$$

for all $p+q \le n$. But we have

$$(p-n+s-1) + (q-n+s-1) = p+q-2n+2s-2 \le 2s-n-2 \le s-r-2$$

and hence $h^{p-n+s-1,q-n+s-1}(Z \times \mathbb{P}^{r-1}) = 0$ for all $(p, q) \in I$ by the above remark.

Further,

$$l^{r,s}(X') \equiv l^{r,s}(X) + h^{r-1,s-1}(Z \times \mathbb{P}^{r-1}) = l^{r,s}(X) + 1 \pmod m$$

since $s-r \le (r-1)+(s-1) \le s+r-2$ and $|r-s| = s-r$.

Finally, $r+s < p+q$ implies $(p-1)+(q-1) > s+r-2$, while $r+s = p+q$ and $s < q$ imply $|p-q| > s-r$, so we have $h^{p-1,q-1}(Z \times \mathbb{P}^{r-1}) = 0$ in both cases and thus

$$l^{p,q}(X') \equiv l^{p,q}(X) + h^{p-1,q-1}(Z \times \mathbb{P}^{r-1}) = l^{p,q}(X) \pmod m$$

for all $(p, q) \in I$ with $(r, s) \prec (p, q)$. □

Proof of Theorem 5. The statement is an immediate consequence of applying Proposition 7 inductively $t_{p,q}$ times to each $(p, q) \in I$ in the descending order induced by $\prec$, where $t_{p,q} \equiv l^{p,q} - l^{p,q}(X_{p,q}) \pmod m$ and $X_{p,q}$ is the variety obtained in the previous step. □

4. Polynomial relations

The following principle seems to be classical.

Lemma 8. *Let $N \ge 1$ and $S \subset \mathbb{Z}^N$ be a subset such that its reduction modulo m is the whole of $(\mathbb{Z}/m\mathbb{Z})^N$ for infinitely many integers $m \ge 2$. If $f \in \mathbb{C}[x_1, \dots, x_N]$ is a polynomial vanishing on S, then $f = 0$.*

Proof. Let $f \in \mathbb{C}[x_1, \dots, x_N]$ be a nonzero polynomial vanishing on S. By choosing a $\mathbb{Q}$-basis of $\mathbb{C}$ and a $\mathbb{Q}$-linear projection $\mathbb{C} \to \mathbb{Q}$ which sends a nonzero coefficient of f to 1, we see that we may assume that the coefficients of f are rational, hence even integral. Since $f \neq 0$, there exists a point $z \in \mathbb{Z}^N$ such that $f(z) \neq 0$. Choose an integer $m \geq 2$ from the assumption which does not divide $f(z)$. Then $f(z) \not\equiv 0 \pmod{m}$. However, we have $z \equiv s \pmod{m}$ for some $s \in S$ and thus $f(z) \equiv f(s) = 0 \pmod{m}$, because $f \in \mathbb{Z}[x_1, \dots, x_N]$. This is a contradiction. □

Proof of Corollary 3. This follows by applying Lemma 8 to the set S of possible Hodge diamonds, where we consider only a nonredundant quarter of the diamond to take the Hodge symmetries into account. Theorem 2 guarantees that the reductions of S modulo m are surjective even for all integers $m \geq 2$. □

In the same way Theorem 2 implies Corollary 3, Theorem 5 yields the following.

Corollary 9. *There are no nontrivial polynomial relations among the inner Hodge numbers of all smooth complex projective varieties in any given birational equivalence class.*

Acknowledgements

The second named author thanks J. Kollár and D. Kotschick for independently making him aware of Kollár's question (answered in Corollary 3 above), which was the starting point of this paper. The authors are grateful to the referees for useful suggestions. This work is supported by the DFG project "Topologische Eigenschaften von algebraischen Varietäten" (project no. 416054549).

References

[Arapura 2016] D. Arapura, "Geometric Hodge structures with prescribed Hodge numbers", pp. 414–421 in *Recent advances in Hodge theory*, edited by M. Kerr and G. Pearlstein, Lond. Math. Soc. Lecture Note Ser. **427**, Cambridge Univ. Press, 2016. MR Zbl

[Hunt 1989] B. Hunt, "Complex manifold geography in dimension 2 and 3", *J. Differential Geom.* **30**:1 (1989), 51–153. MR Zbl

[Kotschick and Schreieder 2013] D. Kotschick and S. Schreieder, "The Hodge ring of Kähler manifolds", *Compos. Math.* **149**:4 (2013), 637–657. MR Zbl

[Schreieder 2015] S. Schreieder, "On the construction problem for Hodge numbers", *Geom. Topol.* **19**:1 (2015), 295–342. MR Zbl

[Simpson 2004] C. Simpson, "The construction problem in Kähler geometry", pp. 365–402 in *Different faces of geometry*, edited by S. Donaldson et al., Int. Math. Ser. **3**, Springer, 2004. MR Zbl

[Voisin 2002] C. Voisin, *Hodge theory and complex algebraic geometry, I*, Cambridge Stud. Adv. Math. **76**, Cambridge Univ. Press, 2002. MR Zbl

Communicated by János Kollár
Received 2019-03-13 Revised 2019-06-13 Accepted 2019-07-29

paulsen@math.lmu.de Mathematisches Institut, LMU München, Germany

schreieder@math.lmu.de Mathematisches Institut, LMU München, Germany

Guidelines for Authors

Authors may submit manuscripts in PDF format on-line at the Submission page at the ANT website.

Originality. Submission of a manuscript acknowledges that the manuscript is original and and is not, in whole or in part, published or under consideration for publication elsewhere. It is understood also that the manuscript will not be submitted elsewhere while under consideration for publication in this journal.

Language. Articles in *ANT* are usually in English, but articles written in other languages are welcome.

Length There is no a priori limit on the length of an *ANT* article, but *ANT* considers long articles only if the significance-to-length ratio is appropriate. Very long manuscripts might be more suitable elsewhere as a memoir instead of a journal article.

Required items. A brief abstract of about 150 words or less must be included. It should be self-contained and not make any reference to the bibliography. If the article is not in English, two versions of the abstract must be included, one in the language of the article and one in English. Also required are keywords and subject classifications for the article, and, for each author, postal address, affiliation (if appropriate), and email address.

Format. Authors are encouraged to use LaTeX but submissions in other varieties of TeX, and exceptionally in other formats, are acceptable. Initial uploads should be in PDF format; after the refereeing process we will ask you to submit all source material.

References. Bibliographical references should be complete, including article titles and page ranges. All references in the bibliography should be cited in the text. The use of BibTeX is preferred but not required. Tags will be converted to the house format, however, for submission you may use the format of your choice. Links will be provided to all literature with known web locations and authors are encouraged to provide their own links in addition to those supplied in the editorial process.

Figures. Figures must be of publication quality. After acceptance, you will need to submit the original source files in vector graphics format for all diagrams in your manuscript: vector EPS or vector PDF files are the most useful.

Most drawing and graphing packages (Mathematica, Adobe Illustrator, Corel Draw, MATLAB, etc.) allow the user to save files in one of these formats. Make sure that what you are saving is vector graphics and not a bitmap. If you need help, please write to graphics@msp.org with details about how your graphics were generated.

White space. Forced line breaks or page breaks should not be inserted in the document. There is no point in your trying to optimize line and page breaks in the original manuscript. The manuscript will be reformatted to use the journal's preferred fonts and layout.

Proofs. Page proofs will be made available to authors (or to the designated corresponding author) at a Web site in PDF format. Failure to acknowledge the receipt of proofs or to return corrections within the requested deadline may cause publication to be postponed.

Algebra & Number Theory

Volume 13 No. 10 2019