RIGID LOCAL SYSTEMS WITH MONODROMY GROUP THE CONWAY GROUP Co_3

NICHOLAS M. KATZ, ANTONIO ROJAS-LEÓN, AND PHAM HUU TIEP

Abstract. We first develop some basic facts about certain sorts of rigid local systems on the affine line in characteristic $p > 0$. We then apply them to exhibit a number of rigid local systems of rank 23 on the affine line in characteristic $p = 3$ whose arithmetic and geometric monodromy groups are the Conway group Co_3 in its orthogonal irreducible representation of degree 23.

Contents

Introduction

In the first section, we recall the general set up, and some basic results. In the second section, we generalize the criteria of [R-L, Thm. 1] and [Ka-RLSA, 5.1] for finite (arithmetic and geometric) monodromy to more general local systems. In the third section, we apply these criteria to show that certain local systems have finite (arithmetic and geometric) monodromy groups. In the fourth section, we show that the finite monodromy groups in question are the Conway group Co_3 in its 23-dimensional irreducible orthogonal representation.

The second author was partially supported by MTM2016-75027-P (Ministerio de Economía y Competitividad) and FEDER. The third author gratefully acknowledges the support of the NSF (grant DMS-1840702).

1. The basic set up, and general results

We fix a prime number p, a prime number $\ell \neq p$, and a nontrivial $\overline{\mathbb{Q}_\ell}^\times$-valued additive character ψ of $\mathbb{F}_p$. For $k/\mathbb{F}_p$ a finite extension, we denote by ψ_k the nontrivial additive character of k given by $\psi_k := \psi \circ \mathrm{Trace}_{k/\mathbb{F}_p}$. In perhaps more down to earth terms, we fix a nontrivial $\mathbb{Q}(\mu_p)^\times$-valued additive character ψ, of $\mathbb{F}_p$, and a field embedding of $\mathbb{Q}(\mu_p)$ into $\overline{\mathbb{Q}_\ell}$ for some $\ell \neq p$.

Given an integer $D \geq 3$ which is prime to p, a finite extension $k/\mathbb{F}_p$, and a polynomial $f(x) \in k[x]$ of degree D, we form the local system $\mathcal{F}_{p,D,f,\mathbb{1}}$ on $\mathbb{A}^1/k$ whose trace function is given as follows: for L/k a finite extension, at L-valued points $t \in \mathbb{A}^1(L) = L$, is given by

$$t \mapsto -\sum_{x \in L} \psi_L(f(x) + tx).$$

This is a geometrically irreducible rigid local system on $\mathbb{A}^1$, being the Fourier Transform of the rank one local system $\mathcal{L}_{\psi(f(x))}$. It has rank $D-1$, it is totally wild at ∞, and each of its $D-1$ $I(\infty)$-slopes is $D/(D-1)$. It is pure of weight one. [When $f(x)$ is x^D, it is the local system $\mathcal{F}(\mathbb{F}_p, \psi, \mathbb{1}, D)$ of [Ka-RLSA].]

Suppose in addition we are given a **nontrivial** character χ of $k^\times$. For L/k a finite extension, we obtain a nontrivial character χ_L of $L^\times$ by defining $\chi_L := \chi \circ \mathrm{Norm}_{L/k}$. We then form the local system $\mathcal{F}_{p,D,f,\chi}$ on $\mathbb{A}^1/k$ whose trace function is given as follows: for L/k a finite extension, at L-valued points $t \in \mathbb{A}^1(L) = L$, is given by

$$t \mapsto -\sum_{x \in L} \psi_L(f(x) + tx)\chi_L(x).$$

This too is a geometrically irreducible rigid local system, being the Fourier Transform of the rank one local system $\mathcal{L}_{\psi(f(x))} \otimes \mathcal{L}_{\chi(x)}$. It has rank D. Its $I(\infty)$ representation is the direct sum of the tame character $\mathcal{L}_{\overline{\chi}(x)}$ with a totally wild representation of rank $D-1$, each of whose $D-1$ $I(\infty)$-slopes is $D/(D-1)$ [Lau, Thm. 2.4.3]. It is pure of weight one. [When $f(x)$ is x^D, it is the local system $\mathcal{F}(\mathbb{F}_p, \psi, \chi, D)$ of [Ka-RLSA].]

Lemma 1.1. (Primitivity Lemma) *We have the following results.*

(i) *If both D and $D-1$ are prime to p, the local system $\mathcal{F}_{p,D,f,\mathbb{1}}$ is not geometrically induced, i.e., there is no triple $(U, \pi, \mathcal{H})$ consisting of a connected smooth curve $U/\overline{k}$, a finite etale map $f : U \to \mathbb{A}^1/\overline{k}$ of degree $d \geq 2$, and a local system $\mathcal{H}$ on U such that there exists an isomorphism of $\pi_\star\mathcal{H}$ with (the pullback to $\mathbb{A}^1/\overline{k}$ of) $\mathcal{F}_{p,D,f,\mathbb{1}}$.*

(ii) *When D is prime to p, then for any nontrivial χ, the local system $\mathcal{F}_{p,D,f,\chi}$ is not geometrically induced.*

Proof. In case (i), our local system is an Airy sheaf (the Fourier transform of a nonconstant lisse sheaf on $\mathbb{A}^1$ of rank one). By a result [Such, 11.1] if an Airy sheaf is induced, it is Artin-Schreier induced, so has rank divisible by p.

For (ii), we argue as follows. If such a triple exists, then we have an equality of Euler characteristics

$$EP(U,\mathcal{H}) = EP(\mathbb{A}^1/\overline{k}, \pi_\star\mathcal{H}) = EP(\mathbb{A}^1/\overline{k}, \mathcal{F}_{p,D,f,\chi}).$$

Denote by X the complete nonsingular model of U, and by g_X its genus. Then π extends to a finite flat map of X to $\mathbb{P}^1$, and the Euler-Poincaré formula gives

$$EP(U,\mathcal{H}) = \mathrm{rank}(\mathcal{H})(2-2g_X - \#(\pi^{-1}(\infty))) - \sum_{w\in\pi^{-1}-(\infty)} \mathsf{Swan}_w(\mathcal{H}),$$

$$EP(\mathbb{A}^1/\overline{k}, \mathcal{F}_{p,D,f,\chi}) = \mathrm{rank}(\mathcal{F}_{p,D,f,\chi}) - \mathsf{Swan}_\infty(\mathcal{F}_{p,D,f,\chi}) = D - D = 0.$$

So we have the equality

$$0 = \mathrm{rank}(\mathcal{H})(2-2g_X - \#(\pi^{-1}(\infty))) - \sum_{w\in\pi^{-1}(\infty)} \mathsf{Swan}_w(\mathcal{H}).$$

We first bound the genus g_X. We must have $g_X \leq 0$, otherwise the factor $2-2g_X-\#(\pi^{-1}(\infty))$ is ≤ -1, and the right hand side is strictly negative.

Thus $g_X = 0$, and we have

$$0 = \mathrm{rank}(\mathcal{H})(2 - \#(\pi^{-1}(\infty))) - \sum_{w\in\pi^{-1}(\infty)} \mathsf{Swan}_w(\mathcal{H}).$$

If $\#(\pi^{-1}(\infty)) = 1$, then U is $\mathbb{P}^1 \setminus (\text{one point}) \cong \mathbb{A}^1$, and so π is a finite etale map of $\mathbb{A}^1$ to itself of degree > 1. But any such map has degree divisible by p. Indeed, when the map is given by the polynomial $F(x)$, the hypothesis is that for every $t \in \overline{k}$, the two equations $F(x) = t, F'(x) = 0$ have no common solution. If F' had a zero, say a, then a would be a solution of $F(x) = F(a), F'(x) = 0$. Thus F' has no zeroes, so is some nonzero constant A, and hence $F(x)$ is of the form $G(x)^p + Ax$.

We cannot have $\#(\pi^{-1}(\infty)) \geq 3$, otherwise the factor $2-\#(\pi^{-1}(\infty))$ is strictly negative, and the right side is then strictly negative. It remains to treat the case when $\#(\pi^{-1}(\infty)) = 2$ (and $g_X = 0$). Throwing the two points to 0 and ∞, we have a finite etale map

$$\pi : \mathbb{G}_m \to \mathbb{A}^1.$$

The equality of EP's now gives

$$0 = \mathsf{Swan}_0(\mathcal{H}) + \mathsf{Swan}_\infty(\mathcal{H}).$$

Thus $\mathcal{H}$ is lisse on $\mathbb{G}_m$ and everywhere tame, so a successive extension of lisse, everywhere tame sheaves of rank one. But $\pi_\star\mathcal{H}$ is irreducible, so $\mathcal{H}$ must itself be irreducible, hence of rank one, and either $\overline{\mathbb{Q}_\ell}$ or an $\mathcal{L}_\rho$. [It cannot be $\overline{\mathbb{Q}_\ell}$, because $\pi_\star\overline{\mathbb{Q}_\ell}$ is not irreducible when π has degree > 1; by adjunction $\pi_\star\overline{\mathbb{Q}_\ell}$ contains $\overline{\mathbb{Q}_\ell}$.] Now consider the maps induced by π on punctured formal neighborhoods

$$\pi(0) : \mathbb{G}_m(0) \to \mathbb{A}^1(\infty), \quad \pi(\infty) : \mathbb{G}_m(\infty) \to \mathbb{A}^1(\infty).$$

The $I(\infty)$-representation of $\mathcal{F}_{p,D,f,\chi}$ is then the direct sum

$$\pi(0)_\star\mathcal{L}_\rho \oplus \pi(\infty)_\star\mathcal{L}_\rho.$$

Denote by d_0 and d_∞ their degrees. For any tame $\mathcal{L}_\Lambda$, we have

$$\pi(0)^\star\mathcal{L}_\Lambda \cong \mathcal{L}_{\Lambda^{d_0}}, \quad \pi(\infty)^\star\mathcal{L}_\Lambda \cong \mathcal{L}_{\Lambda^{d_\infty}}.$$

Since the tame character group is divisible, there exist Λ_0 with $\Lambda_0^{d_0} = \rho$ (in fact, as many as the prime to p part n_0 of $d_0 = n_0 \times (\text{a power of } p)$), and there exist Λ_∞ with $\Lambda_\infty^{d_\infty} = \rho$ (in fact, as many as the prime to p part n_∞ of $d_\infty = n_\infty \times (\text{a power of } p)$,

Thus if $\mathcal{F}_{p,D,f,\chi}$ were induced, its $I(\infty)$ representation would contain at least two tame characters. □

Let k be a finite extension of $\mathbb{F}_p$, $\ell \neq p$, U/k a smooth, geometrically connected k-scheme of relative dimension ≥ 0, and $\mathcal{G}$ a $\overline{\mathbb{Q}_\ell}$ local system on U of rank $d \geq 1$. Viewing $\mathcal{G}$ as a representation of $\pi_1(U)$, say

$$\rho_{\mathcal{G}} : \pi_1(U) \to \mathrm{GL}_d(\overline{\mathbb{Q}_\ell}),$$

we get its arithmetic monodromy group G_{arith}, defined to be the Zariski closure of the image of $\pi_1(U)$. Inside $\pi_1(U)$ we its normal subgroup $\pi_1^{geom}(U) := \pi_1(U \otimes_k \overline{k})$. The Zariski closure of the image of $\pi_1^{geom}(U)$ is the geometric monodromy group G_{geom}. Thus we have

$$G_{geom} \lhd G_{arith} \subset \mathrm{GL}_d(\overline{\mathbb{Q}_\ell}).$$

When we apply this general machine to the local system $\mathcal{F}_{p,D,f,\mathbb{1}}$ on $\mathbb{A}^1/k$, we get its

$$G_{geom} \lhd G_{arith} \subset \mathrm{GL}_{D-1}(\overline{\mathbb{Q}_\ell}).$$

Similarly, for any nontrivial χ, when we apply the general machine to the local system $\mathcal{F}_{p,D,f,\chi}$ on $\mathbb{A}^1/k$, we get its

$$G_{geom} \lhd G_{arith} \subset \mathrm{GL}_D(\overline{\mathbb{Q}_\ell}).$$

Lemma 1.2. (p-subgroups of G_{geom}) *Suppose both $D \geq 3$ and $D-1$ are prime to p. Denote by f the multiplicative order of p in $(\mathbb{Z}/(D-1)\mathbb{Z})^\times$, so that $\mathbb{F}_{p^f}$ is the extension $\mathbb{F}_p(\mu_{D-1})$ of $\mathbb{F}_p$ obtained by adjoining the $D-1$ roots of unity. Then for the particular local systems $\mathcal{F}_{p,D,x^D,\mathbb{1}}$ or $\mathcal{F}_{p,D,x^D,\chi}$ with any nontrivial χ, the image in G_{geom} of the wild inertia group $P(\infty)$ is isomorphic to (the additive group of) $\mathbb{F}_{p^f}$.*

Proof. In all cases, the local system, restricted to $\mathbb{G}_m$, descends through the D'th power map. For $\mathcal{F}_{p,D,x^D,\mathbb{1}}$, the descent is given explicitly in terms of trace functions as

$$t \mapsto -\sum_{x\in k} \psi_k(x^D/t + x).$$

For $\mathcal{F}_{p,D,x^D,\chi}$, we must first choose a character Λ with $\Lambda^D = \overline{\chi}$. Then the descent is given explicitly interms of trace function as

$$t \mapsto -\sum_{x\in L^\times} \Lambda_L(t)\psi_k(x^D/t + x)\chi_L(x).$$

In fancier terms, the first descent is to a Kloosterman sheaf of rank $D-1$, the second is to a hypergeometric sheaf of type $(D, 1)$, cf. [Ka-RLSA, 2.1].

In all cases, the wild part W of the $I(\infty)$ representation has rank $D-1$ and all slopes $1/(D-1)$. Because $D-1 \geq 2$, one knows [Ka-ESDE, 8.6.3] that W is unique up to tensoring with a tame character and performing a multiplicative translation. Thus the underlying $P(\infty)$-representation is unique up to a multiplicative translation, which does not change its image in G_{geom}. Because $D-1$ is prime to p, we obtain one such W by forming the direct image by $D-1$ power

$$W := [D-1]_\star \mathcal{L}_{\psi(x)}.$$

Because $D-1$ is prime to p, the image of $P(\infty)$ does not change if we pass to the pullback

$$[D-1]^\star W = [D-1]^\star[D-1]_\star \mathcal{L}_{\psi(x)} \cong \bigoplus_{\zeta\in\mu_{D-1}} \mathcal{L}_{\psi(\zeta x)}.$$

In other words, the image of $P(\infty)$ is the abelian group whose character group consists of all monomials

$$\otimes_{\zeta\in\mu_{D-1}} \mathcal{L}_{\psi(\zeta x)}^{\otimes n_\zeta} = \mathcal{L}_{\psi(\sum_{\zeta\in\mu_{D-1}} n_\zeta \zeta x)}.$$

as each n_ζ runs over $\mathbb{Z}/p\mathbb{Z}$. This character group is thus the subring $\mathbb{F}_p[\mu_{D-1}] \subset \mathbb{F}_{p^f}$ consisting of all $\mathbb{F}_p$-linear combinations of elements of μ_{D-1}. But this subring, being a finite integral domain, is itself a field.

It lies in $\mathbb{F}_{p^f}$, and contains μ_{D-1}, so it is $\mathbb{F}_{p^f}$. One knows that (by the trace), $\mathbb{F}_{p^f}$ is its own Pontrayagin dual. □

2. Criteria for finite monodromy

We first recall the basic underlying result, cf [Ka-ESDE, 8.14]. [It is stated there for a local system on an open curve, but the "on a curve" hypothesis never enters the proof. Also, the exact rule of the hypothesis of geometric irreducibility is less clear than it might be, cf. Remark 2.2 below.

Let k be a finite extension of $\mathbb{F}_p$, $\ell \neq p$, U/k a smooth, geometrically connected k-scheme of relative dimension ≥ 0, and $\mathcal{G}$ a $\overline{\mathbb{Q}_\ell}$ local system on U of rank $d \geq 1$. We have its geometric and arithmetic monodromy groups

$$G_{geom} \lhd G_{arith} \subset \mathrm{GL}_d(\overline{\mathbb{Q}_\ell}).$$

Proposition 2.1. *Suppose we have $(k, \ell, U, \mathcal{G})$ as above. Suppose further that $\mathcal{G}$ is pure of weight zero for all embeddings of $\overline{\mathbb{Q}_\ell}$ into $\mathbb{C}$. Consider the following four conditions.*

(a) *G_{arith} is finite.*
(b) *All traces of $\mathcal{G}$ are algebraic integers. More precisely, for every finite extension L/k, and for every point $u \in U(L)$, $\mathrm{Trace}(Frob_{L,u}|\mathcal{G})$ is an algebraic integer.*
(c) *G_{geom} is finite.*
(d) *$\det(\mathcal{G})$ is arithmetically of finite order.*

Then we have the implications

$$\text{(a)} \implies \text{(b)} \implies \text{(c)}, \quad \text{(b)} \implies \text{(d)},$$

and if $\mathcal{G}$ is geometrically irreducible, we have (a) $\iff$ (b) $\iff$ (c).

Proof. The implications (a) $\implies$ (b) and (a) $\implies$ (c) are both obvious.

We next show that (b) $\implies$ (c) and (b) $\implies$ (d). If (b) holds, then all the eigenvalues of each Frobenius are algebraic integers which, by purity, have absolute value 1 at all archimedean places, hence are roots of unity. Because $\mathcal{G}$ is realizable over some finite extension E_λ of $\mathbb{Q}_\ell$, each of these roots of unity lies in a extension of E_λ of degree at most the rank of $\mathcal{G}$. As there are only finitely many such extensions inside $\overline{\mathbb{Q}_\ell}$, all eigenvalues are roots of unity in a fixed finite extension of $\mathbb{Q}_\ell$, so are all N'th roots of unity for some N. Applying this same argument to the rank one local system $\det(\mathcal{G})$, we see that $\det(\mathcal{G})^{\otimes N}$ is trivial, i.e. we see that (b) $\implies$ (d). By Chebotarev and Zariski density, every $\gamma \in G_{arith}$ has γ^N unipotent. In particular, every element in G_{geom}, and

hence every element in the identity component G^0_{geom} has N'th power unipotent. By Deligne [De-Weil II, 1.3.8 and 3.4.1 (iii)], G^0_{geom} is a semisimple algebraic group. Looking at elements of a maximal torus, we see that G^0_{geom} has rank 0, hence G^0_{geom} is trivial and thus G_{geom} is finite.

When $\mathcal{G}$ is geometrically irreducible, the implication (c) $\Longrightarrow$ (a), using (d), is proven in [Ka-ESDE, 8.14.3.1]. □

Remark 2.2. Here is an example to show that geometric irreducibility is needed to prove that (b) $\Longrightarrow$ (a). Take any U/k, and take on it the pullback from $Spec(k)$ of the geometrically constant local system β^{deg} for β the upper unipotent matrix $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Then all Frobenius eigenvalues are 1, G_{geom} is trivial, but G_{arith} is the upper unipotent subgroup $\begin{pmatrix} 1 & \star \\ 0 & 1 \end{pmatrix}$ of $SL(2)$.

On the other hand, suppose (b) holds. If we pass from $\mathcal{G}$ viewed as a representation of π_1^{arith}, to its semisimplification $\mathcal{G}^{ss}$, (which has the same trace function as $\mathcal{G}$), then $G_{arith,\mathcal{G}^{ss}}$ is reductive. Then the fact that every element in this group has N'power unipotent shows that the identity component $G^0_{arith,\mathcal{G}^{ss}}$ is trivial (look at a maximal torus), and hence $G_{arith,\mathcal{G}^{ss}}$ is finite.

We now define the sort of multi-parameter local systems it will be convenient to work with. We fix an integer $D \geq 3$ prime to p, and a sequence of integers of length $r \geq 1$,

$$1 = d_1 < d_2 < \ldots < d_r < D,$$

each of which is itself prime to p. [Because of Artin-Schreier reduction, requiring the d_i to be prime to p is no loss of generality.] We form the local system $\mathcal{F}(p, D, d_1, \ldots, d_r, \mathbb{1})$ on $\mathbb{A}^{r-1}$ whose trace function is as follows: for $K/\mathbb{F}_p$ a finite extension, and $(t_, \ldots, t_r) \in \mathbb{A}^r(K)$, the trace function is

$$(t_, \ldots, t_r) \mapsto -\sum_{x \in K} \psi_K(x^D + \sum_i t_i x^{d_i}).$$

When p is odd, we also form the local system $\mathcal{F}(p, D, d_1, \ldots, d_r, \chi_2)$ on $\mathbb{A}^{r-1}$ whose trace function is as follows: for $K/\mathbb{F}_p$ a finite extension, and $(t_, \ldots, t_r) \in \mathbb{A}^r(K)$, the trace function is

$$(t_, \ldots, t_r) \mapsto -\sum_{x \in K^\times} \psi_K(x^D + \sum_i t_i x^{d_i})\chi_{2,K}(x).$$

Because $d_1 = 1$, these local systems are geometrically irreducible (indeed, for $r = 1$ these are $\mathcal{F}(p, D, x^D, \mathbb{1})$ and $\mathcal{F}(p, D, x^D, \chi_2)$). If $r \geq$

2, their pullbacks to $\mathbb{A}^1$ by freezing $t_2 = \ldots = t_r = 0$ are $\mathcal{F}(p, D, x^D, \mathbb{1})$ and $\mathcal{F}(p, D, x^D, \chi_2)$. They are pure of weight one, for all embeddings of $\overline{\mathbb{Q}_\ell}$ into $\mathbb{C}$. Moreover, their traces lie in $\mathbb{Z}[\zeta_p]$.

For each of them, we now fix a version of a half Tate twist as follows: we choose an algebraic integer α which is (some root of unity)$\sqrt{p}$, typically some fourth root of p^2.

Using our chosen α, we then define

$$\mathcal{G}(p, D, d_1, \ldots, d_r, \mathbb{1}) := \mathcal{F}(p, D, d_1, \ldots, d_r, \mathbb{1}) \otimes (1/\alpha)^{deg},$$

and, when p is odd,

$$\mathcal{G}(p, D, d_1, \ldots, d_r, \chi_2) := \mathcal{F}(p, D, d_1, \ldots, d_r, \chi_2) \otimes (1/\alpha)^{deg}.$$

The local systems $\mathcal{G}_{p,D,f,\mathbb{1}}$ and, when p is odd, $\mathcal{G}_{p,D,f,\chi_2}$, are pure of weight zero. Their determinants are arithmetically of finite order, cf. the proof of [Ka-RL, Lemma 1.1].

For later use, we record the following facts about autoduality.

Lemma 2.3. *Suppose that D and all the d_i are* **odd**. *Then there is a preferred choice of α, as follows.*

(1) *For α either choice of $\sqrt{p}$, $\mathcal{G}(p, D, d_1, \ldots, d_r, \mathbb{1})$ has*
$$G_{geom} \lhd G_{arith} \subset \mathrm{Sp}_{D-1}(\overline{\mathbb{Q}_\ell}).$$

(2) *If p is odd, write $D = 2\delta+1$. Then for $\alpha := -\chi_2((-1)^\delta D)g(\psi, \chi_2)$ ($g(\psi, \chi_2)$ the quadratic Gauss sum over $\mathbb{F}_p$), $\mathcal{G}(p, D, d_1, \ldots, d_r, \chi_2)$ has*
$$G_{geom} \lhd G_{arith} \subset \mathrm{SO}_D(\overline{\mathbb{Q}_\ell}).$$

(3) *Denote by $\mathbb{Q}(\zeta_p)^+$ the real subfield of $\mathbb{Q}(\zeta_p)^+$. In case (1), the traces attained lie in $\mathbb{Q}(\zeta_p)^+(\sqrt{p})$. In case (2), they lie in $\mathbb{Q}(\zeta_p)^+$.*

Proof. Assertion (1) is Poincaré duality. Assertion (2) is proved in [Ka-NG2, 1.7]. Assertion (3) is obvious from applying complex conjugation to the formulas for the traces. □

The local system $\mathcal{G}(p, D, d_1, \ldots, d_r, \mathbb{1})$ on $\mathbb{A}^r/\mathbb{F}_p$ has its
$$G_{geom} \lhd G_{arith} \subset \mathrm{GL}_{D-1}(\overline{\mathbb{Q}_\ell}).$$

Similarly, when p is odd, the local system $\mathcal{G}(p, D, d_1, \ldots, d_r, \chi_2)$ on $\mathbb{A}^r/\mathbb{F}_p$ has its
$$G_{geom} \lhd G_{arith} \subset \mathrm{GL}_D(\overline{\mathbb{Q}_\ell}).$$

We now apply 2.1 to these local systems.

Proposition 2.4. *The following conditions are equivalent.*

(a) *$\mathcal{G}(p, D, d_1, \ldots, d_r, \mathbb{1})$ has finite G_{geom}.*

(a-bis) $\mathcal{F}(p, D, d_1, \dots, d_r, \mathbb{1})$ *has finite* G_{geom}.
(b) $\mathcal{G}(p, D, d_1, \dots, d_r, \mathbb{1})$ *has finite* G_{arith}.
(c) *All traces of* $\mathcal{G}(p, D, d_1, \dots, d_r, \mathbb{1})$ *are algebraic integers.*
When p *is odd, we have these same equivalences for* $\mathcal{G}(p, D, d_1, \dots, d_r, \chi_2)$.

We now perform two successive reduction steps. The first is to pull back these local systems from $\mathbb{A}^r$ to $\mathbb{G}_m^r$, i.e., requiring the coefficients t_i to all be invertible.

Lemma 2.5. *The following conditions are equivalent.*
(a) $\mathcal{G}(p, D, d_1, \dots, d_r, \mathbb{1})$ *has finite* G_{arith}.
(b) *The pullback of* $\mathcal{G}(p, D, d_1, \dots, d_r, \mathbb{1})$ *to* $\mathbb{G}_m^r$ *has finite* G_{arith}.
If p *is invertible, the same equivalence holds for* $\mathcal{G}(p, D, d_1, \dots, d_r, \chi_2)$.

Proof. That (a) implies (b) is obvious. Because $\mathbb{G}_m^r$ is a dense open set of $\mathbb{A}^r$, $\pi_1(\mathbb{G}_m^r)$ maps onto $\pi_1(\mathbb{A}^r)$, hence (b) implies (a). □

We now form local systems $\mathcal{G}_{big}(p, D, d_1, \dots, d_r, \mathbb{1})$ and, if p is odd, $\mathcal{G}_{big}(p, D, d_1, \dots, d_r, \chi_2)$ on $\mathbb{G}_m^{r+1}$, by letting the coefficient of x^D also vary over invertible scalars. Thus the trace function of $\mathcal{G}_{big}(p, D, d_1, \dots, d_r, \mathbb{1})$ is

$$(t_1, \dots, t_{r+1}) \in \mathbb{G}_m(K)^{r+1} \mapsto \sum_{x \in K} \psi_K(t_{r+1}x^D + \sum_i t_i x^{d_i})/\alpha^{\deg(K/\mathbb{F}_p)}.$$

When p is odd, the trace function of $\mathcal{G}_{big}(p, D, d_1, \dots, d_r, \chi_2)$ is

$$(t_1, \dots, t_{r+1}) \in \mathbb{G}_m(K)^{r+1} \mapsto \sum_{x \in K^\times} \psi_K(t_{r+1}x^D + \sum_i t_i x^{d_i})\chi_{2,K}(x)/\alpha^{\deg(K/\mathbb{F}_p)}.$$

Lemma 2.6. *The following conditions are equivalent.*
(a) $\mathcal{G}_{big}(p, D, d_1, \dots, d_r, \mathbb{1})$ *on* $\mathbb{G}_m^{r+1}$ *has finite* G_{arith}.
(b) *The pullback of* $\mathcal{G}(p, D, d_1, \dots, d_r, \mathbb{1})$ *to* $\mathbb{G}_m^r$ *has finite* G_{arith}.
If p *is invertible, the same equivalence holds with* $\mathbb{1}$ *replaced by* χ_2.

Proof. In both cases, it is obvious that (a) implies (b), since the second local system is the pullback of the first to the locus $t_{r+1} = 1$. To show that (b) implies (a), we argue as follows. Over a finite extension K of $\mathbb{F}_p$, if we make the substitution $x \mapsto \lambda x$ with $\lambda \in K^\times$, the sum

$$\sum_{x \in K} \psi_K(x^D + \sum_i t_i x^{d_i})/\alpha^{\deg(K/\mathbb{F}_p)}$$

is equal to the sum

$$\sum_{x \in K} \psi_K(\lambda^d x^D + \sum_i \lambda^{d_i} t_i x^{d_i})/\alpha^{\deg(K/\mathbb{F}_p)}.$$

After the change of variable $t_i \mapsto t_i/\lambda^{d_i}$, this sum is

$$\sum_{x\in K} \psi_K(\lambda^d x^D + \sum_i t_i x^{d_i})/\alpha^{\deg(K/\mathbb{F}_p)},$$

still an algebraic integer. In other words, the pullback of $\mathcal{G}_{big}(p, D, d_1, \ldots, d_r, \mathbb{1})$ on $\mathbb{G}_m^{r+1}$ to $\mathbb{G}_m^{r+1}$ by the finite etale galois map

$$(t_1, \ldots, t_r, t_{r+1}) \mapsto (t_1, \ldots, t_r, t_{r+1}^D)$$

has all its traces algebraic integers, hence has finite G_{arith}. But under this finite etale map, the map of π_1's makes the source a subgroup of index D in the target. Thus the G_{arith} for $\mathcal{G}_{big}(p, D, d_1, \ldots, d_r, \mathbb{1})$ contains a finite group as a subgroup of finite index, so is itself finite.

When p is odd, and $\chi = \chi_2$, apply the identical argument. In this case, the $x \mapsto \lambda x$ substitution moves the sum by a factor $\chi_2(\lambda) = \pm 1$, so does not change the fact that the sum is an algebraic integer. □

The sums

$$\sum_{x\in K} \psi_K(t_{r+1}x^D + \sum_i t_i x^{d_i})$$

and, when p is odd, the sums

$$\sum_{x\in K^\times} \psi_K(t_{r+1}x^D + \sum_i t_i x^{d_i})\chi_{2,K}(x),$$

lie in $\mathbb{Z}[\zeta_p]$. The quantity α in all cases has $\alpha^4 = p^2$. The field $\mathbb{Q}(\zeta_p)$ has a unique place over p. So these sums will **remain** algebraic integers when divided by $\alpha^{\deg(K/\mathbb{F}_p)}$ if and only if the divided sums be p-integral. Equivalently , whenever K is $\mathbb{F}_q$, and ord_q is the p-adic ord, normalized to have $\mathrm{ord}_q(q) = 1$, we must have

$$\mathrm{ord}_q\left(\sum_{x\in K=\mathbb{F}_q} \psi_K(t_{r+1}x^D + \sum_i t_i x^{d_i})\right) \geq 1/2,$$

and, when p is odd, we must have

$$\mathrm{ord}_q\left(\sum_{x\in K^\times=\mathbb{F}_q^\times} \psi_K(t_{r+1}x^D + \sum_i t_i x^{d_i})\chi_{2,K}(x)\right) \geq 1/2,$$

for every finite extension $K/\mathbb{F}_p$ and every $r+1$ tuple $(t_1, \ldots, t_{r+1}) \in (K^\times)^{r+1}$.

We now give a generalization of [R-L, Theorem 1] to these local systems. In the formulation, we make reference to the ord_q of various Gauss sums over variable $\mathbb{F}_q$. We view these sums as taking values in $\mathbb{Q}_p(\zeta_p)^{nr}$, the maximal unramified extension of $\mathbb{Q}_p(\zeta_p)$ (i.e., we adjoin

to $\mathbb{Q}_p(\zeta_p)$ all roots of unity of order prime to p). This field has a unique p-adic ord.

Theorem 2.7. *We have the following results, in which we write $d_{r+1} := D$.*

(i) *$\mathcal{G}_{big}(p, D, d_1, \dots, d_r, \mathbb{1})$ has finite G_{arith} if and only if the following condtion holds.*

For every finite extension $K = \mathbb{F}_q$ of $\mathbb{F}_p$, and for every $r+1$ tuple of (possibly trivial) multiplicative characters $(\rho_1, \dots, \rho_{r+1})$ of $K^\times$, not all of which are trivial, such that $\prod_i \rho_i^{d_i} = \mathbb{1}$, we have

$$\mathrm{ord}_q(\prod_i g(\psi_K, \rho_i)) \geq 1/2.$$

(ii) *If p is odd, then $\mathcal{G}_{big}(p, D, d_1, \dots, d_r, \chi_2)$ has finite G_{arith} if and only if the following condition holds.*

For every finite extension $K = \mathbb{F}_q$ of $\mathbb{F}_p$, and for every $r+1$ tuple of (possibly trivial) multiplicative characters $(\rho_1, \dots, \rho_{r+1})$ of $K^\times$ such that $\prod_i \rho_i^{d_i} = \chi_{2,K}$, we have

$$\mathrm{ord}_q(\prod_i g(\psi_K, \rho_i)) \geq 1/2.$$

Proof. We first explain the underlying idea. For a fixed $K = \mathbb{F}_q$, we have a function on $(K^\times)^{r+1}$, say

$$F(t_1, \dots, t_{r+1}),$$

whose values lie in $\mathbb{Z}[\zeta_p]$. We wish to show that each divided value $F(t_1, \dots, t_{r+1})/\alpha^{\deg(K/\mathbb{F}_p)}$ remains an algebraic integer, or equivalently that

$$\mathrm{ord}_q(F(t_1, \dots, t_{r+1})) \geq 1/2.$$

For this, we consider the Mellin transform. Recall that for a finite abelian group A, with Pontrayagin dual group

$$A^\vee := \mathrm{Hom}_{\mathrm{groups}}(A, \mathbb{C}^\times),$$

the Mellin transform (also called the Fourier transform) Mellin is an isomorphism

$$\mathsf{Mellin} : \mathrm{Maps}(A, \mathbb{C}) \cong \mathrm{Maps}(A^\vee, \mathbb{C}), \quad F \mapsto \mathsf{Mellin}_F$$

defined as follows. For a function $F : A \to \mathbb{C}$, and a linear character $\chi : A \to \mathbb{C}^\times$,

$$\mathsf{Mellin}_F(\chi) := \sum_{a \in A} F(a)\chi(a).$$

We apply this to the group $(K^\times)^{r+1}$. For each $r+1$ tuple of multiplicative characters $(\rho_1, \dots, \rho_{r+1})$ of $K^\times$, we look at the the sum

$$\mathsf{Mellin}_F(\rho_1, \dots, \rho_{r+1}) := \sum_{(t_1,\dots,t_{r+1})\in(K^\times)^{r+1}} F(t_1, \dots, t_{r+1}) \prod_i \rho_i(t_i).$$

We can recover F from Mellin_F by usual Mellin inversion, which involves division by $(q-1)^{r+1}$, a quantity prime to p. So it suffices to show that each value $\mathsf{Mellin}_F(\rho_1, \dots, \rho_{r+1})$ has $\mathrm{ord}_q \geq 1/2$.

We first treat assertion (i). The function $F(t_1, \dots, t_{r+1})$ at hand is

$$F(t_1, \dots, t_{r+1}) := \sum_{x\in K} \psi_K(t_{r+1}x^D + \sum_{i=1}^{r} t_i x^{d_i}) =$$

$$= \sum_{x\in K} \psi_K(\sum_{i=1}^{r+1} t_i x^{d_i}) = 1 + F^\times(t_1, \dots, t_{r+1}),$$

with

$$F^\times(t_1, \dots, t_{r+1}) := \sum_{x\in K^\times} \psi_K(\sum_{i=1}^{r+1} t_i x^{d_i}).$$

When all the ρ_i are trivial, we have

$$\mathsf{Mellin}_F(\mathbb{1}, \dots, \mathbb{1}) = (q-1)^{r+1} + \mathsf{Mellin}_{F^\times}(\mathbb{1}, \dots, \mathbb{1}),$$

and

$$\mathsf{Mellin}_{F^\times}(\mathbb{1}, \dots, \mathbb{1}) = \sum_{(t_1,\dots,t_{r+1})\in(K^\times)^{r+1}} F^\times(t_1, \dots, t_{r+1}) =$$

$$= \sum_{x\in K^\times} \sum_{(t_1,\dots,t_{r+1})\in(K^\times)^{r+1}} \psi_K(\sum_{i=1}^{r+1} t_i x^{d_i}) =$$

$$= \sum_{x\in K^\times} \prod_i (\sum_{t_i\in K^\times} \psi_K(t_i x^{d_i})).$$

Each of the $r+1$ summands inside the product is equal to -1, because x^{d_i} is nonzero, so $t_i \mapsto \psi_K(t_i x^{d_i})$ is a nontrivial additive character of K, and we sum over the nonzero elements. So we find that

$$\mathsf{Mellin}_{F^\times}(\mathbb{1}, \dots, \mathbb{1}) = (q-1)(-1)^{r+1},$$

and hence

$$\mathsf{Mellin}_F(\mathbb{1}, \dots, \mathbb{1}) = (q-1)^{r+1} + (q-1)(-1)^{r+1},$$

which is divisible by q.

When not all the ρ_i are trivial, the constant term of F dies, and we have

$$\mathsf{Mellin}_F(\rho_1 \dots, \rho_{r+1}) = \mathsf{Mellin}_{F^\times}(\rho_1 \dots, \rho_{r+1}) =$$

$$= \sum_{x\in K^\times} \prod_i \left(\sum_{t_i\in K^\times} \psi_K(t_i x^{d_i})\rho_i(t_i) \right).$$

Here each of the $r+1$ summands inside the product is easily expressed in terms of Gauss sums:

$$\sum_{t_i\in K^\times} \psi_K(t_i x^{d_i})\rho_i(t_i) = \overline{\rho_i}(x^{d_i}) g(\psi_K, \rho_i).$$

So we get

$$\mathsf{Mellin}_F(\rho_1 \ldots, \rho_{r+1}) = (\prod_i g(\psi_K, \rho_i)) \sum_{x\in K^\times} (\prod_i \overline{\rho_i^{d_i}})(x).$$

The sum over $x \in K^\times$ vanishes unless $\prod_i \rho_i^{d_i} = \mathbb{1}$. If $\prod_i \rho_i^{d_i} = \mathbb{1}$, then we get $(q-1)(\prod_i g(\psi_K, \rho_i))$.

The proof of case (ii) is analogous. Here F is already $F^\times$, and the final formula is

$$\mathsf{Mellin}_F(\rho_1 \ldots, \rho_{r+1}) = (\prod_i g(\psi_K, \rho_i)) \sum_{x\in K^\times} (\prod_i \overline{\rho_i^{d_i}})(x)\chi_{2,K}(x).$$

□

We now reformulate the previous Theorem 2.7 in terms of Kubert's V function

$$V : (\mathbb{Q}/\mathbb{Z})_{prime\ to\ p} \to [0,1).$$

For $\mathbb{F}_{p^f}$ a finite extension of $\mathbb{F}_p$, and $x \in (\mathbb{Q}/\mathbb{Z})_{prime\ to\ p}$ with $(p^f-1)x \in \mathbb{Z}$, we have

$$V(x) := \mathrm{ord}_{p^f}(g(\psi_{\mathbb{F}_{p^f}}, \mathsf{Teich}^{-x(p^f-1)})),$$

for

$$\mathsf{Teich}_{p^f} : \mathbb{F}_{p^f}^\times \cong \mu_{p^f-1}(\mathbb{Q}_p^{nr})$$

the Teichmuller character, characterized by the requirement that for any $x \in \mathbb{F}_{p^f}^\times$, $\mathsf{Teich}_{p^f}(x)$ lifts x. For such an x, we have the Stickelberger formula

$$V(x) = (1/f) \sum_{i(\mathrm{mod}\ f)} < p^i x > .$$

It will also be convenient to introduce a slight variant of Kubert's V function, V_{RL}, defined by

$$V_{RL}(x) = V(x) \text{ for } x \neq 0,\ V_{RL}(0) = 1.$$

The advantage of this is that the property of the V function

$$V(x) + V(-x) = 1 \text{ if } x \neq 0$$

becomes the formula

$$V(x) + V_{RL}(-x) = 1, \text{ for all } x.$$

Thus we may reformulate Theorem 2.7 as follows, where we "solve" for x_1 in terms of $(x_2, \dots, x_{r+1})$.

Theorem 2.8. *We have the following results.*

(i) $\mathcal{G}_{big}(p, D, d_1, \dots, d_r, \mathbb{1})$ *has finite* G_{arith} *if and only if the following condtion holds. For every list* $(x_2, \dots, x_{r+1})$ *of elements of* $(\mathbb{Q}/\mathbb{Z})_{prime\ to\ p}$ *which are not all* 0*, we have the inequality*

$$\sum_{i\geq 2} V(x_i) + 1/2 \geq V_{RL}(\sum_{i\geq 2} d_i x_i).$$

(ii) *If* p *is odd, then* $\mathcal{G}_{big}(p, D, d_1, \dots, d_r, \chi_2)$ *has finite* G_{arith} *if and only if the following condtion holds. For every list of elements* $(x_2, \dots, x_{r+1})$ *of elements of* $(\mathbb{Q}/\mathbb{Z})_{prime\ to\ p}$*, we have the inequality*

$$\sum_{i\geq 2} V(x_i) + 1/2 \geq V_{RL}(1/2 + \sum_{i\geq 2} d_i x_i).$$

We now recall the explicit "sum of digits" recipe for V and for V_{RL}, cf. [Ka-RL, Appendix]. For an integer y, and a power p^f of p, we define

$$[y]_{p,f,-}$$

to be the sum of the p-adic digits of the representative of $y \mod p^f - 1$ in $[0, p^f - 2]$, and we define

$$[y]_{p,f}$$

to be the sum of the p-adic digits of the representative of $y \mod p^f - 1$ in $[1, p^f - 1]$. Then we have

$$V\left(\frac{y}{p^f - 1}\right) = \frac{1}{f(p-1)}[y]_{p,f,-},$$

$$V_{RL}\left(\frac{y}{p^f - 1}\right) = \frac{1}{f(p-1)}[y]_{p,f}.$$

With this notation, Theorem 2.8 can be restated as

Theorem 2.9. *We have the following results.*

(i) $\mathcal{G}_{big}(p, D, d_1, \dots, d_r, \mathbb{1})$ *has finite* G_{arith} *if and only if the following condtion holds. For every positive integer* f *and every* r*-tuple of integers* $0 \leq x_2, \dots, x_{r+1} < p^f - 1$ *which are not all* 0*, we have the inequality*

$$\left[\sum_{i=2}^{r+1} d_i x_i\right]_{p,f} \leq \sum_{i=2}^{r+1} [x_i]_{p,f,-} + \frac{f(p-1)}{2} \tag{2.9.1}$$

(ii) *If p is odd, then $\mathcal{G}_{big}(p, D, d_1, \dots, d_r, \chi_2)$ has finite G_{arith} if and only if the following condtion holds. For every positive integer f and every r-tuple of integers $0 \leq x_2, \dots, x_{r+1} < p^f - 1$, we have the inequality*

$$\left[\sum_{i=2}^{r+1} d_i x_i + \frac{p^f - 1}{2}\right]_{p,f} \leq \sum_{i=2}^{r+1} [x_i]_{p,f,-} + \frac{f(p-1)}{2}. \tag{2.9.2}$$

We also have one further criterion that involves the simpler function $[x]_p :=$ sum of the p-adic digits of x. We first prove the following

Lemma 2.10 (Hasse-Davenport relation)**.** *Let f, k be positive integers and $x \in \mathbb{Z}$. Then we have*

$$\left[\frac{p^{fk} - 1}{p^f - 1} x\right]_{p,fk} = k \cdot [x]_{p,f}$$

and

$$\left[\frac{p^{fk} - 1}{p^f - 1} x\right]_{p,fk,-} = k \cdot [x]_{p,f,-}$$

Proof. If $x \equiv y \pmod{p^f - 1}$ then $\frac{p^{fk}-1}{p^f-1} x \equiv \frac{p^{fk}-1}{p^f-1} y \pmod{p^{fk} - 1}$, so it suffices to prove it for $0 \leq x < p^f - 1$ (so $\frac{p^{fk}-1}{p^f-1} x < p^{fk} - 1$). But then the result is clear since the p-adic expansion of $\frac{p^{fk}-1}{p^f-1} x$ is the concatenation of k copies of the p-adic expansion of x (filled with leading 0's so that it has exactly f digits). □

For use below, we recall the following result from [Ka-RL, Prop. 2.2], whose inequalities are used in the proof of Theorem 2.12.

Proposition 2.11. *For strictly positive integers x and y, and any $f \geq 1$, we have:*

(i) $[x + y]_p \leq [x]_p + [y]_p$;
(ii) $[x]_{p,f} \leq [x]_p$;
(iii) $[px]_p = [x]_p$.

Theorem 2.12. *We have the following results.*

(i) *$\mathcal{G}_{big}(p, D, d_1, \dots, d_r, \mathbb{1})$ has finite G_{arith} if and only if there exists some real $A \geq 0$ such that for every positive integer f and every r-tuple of integers $0 \leq x_2, \dots, x_{r+1} < p^f - 1$ which are not all 0, we have the inequality*

$$\left[\sum_{i=2}^{r+1} d_i x_i\right]_p \leq \sum_{i=2}^{r+1} [x_i]_p + \frac{f(p-1)}{2} + A. \tag{2.12.1}$$

(ii) *If p is odd, then $\mathcal{G}_{big}(p, D, d_1, \dots, d_r, \chi_2)$ has finite G_{arith} if and only if there exists some real $A \geq 0$ such that for every positive integer f and every r-tuple of integers $0 \leq x_2, \dots, x_{r+1} < p^f - 1$, we have the inequality*

$$\left[\sum_{i=2}^{r+1} d_i x_i + \frac{p^f - 1}{2}\right]_p \leq \sum_{i=2}^{r+1} [x_i]_p + \frac{f(p-1)}{2} + A. \tag{2.12.2}$$

Proof. We will prove that the hypotheses of this theorem are equivalent to those of Theorem 2.9.

Suppose that there exists $A \geq 0$ such that (2.12.1) holds for every $f \geq 1$ and every $0 \leq x_2, \dots, x_{r+1} < p^f - 1$ which are not all zero. Then $\sum_{i=2}^{r+1} d_i x_i > 0$, and

$$\begin{aligned}\left[\sum_{i=2}^{r+1} d_i x_i\right]_{p,f} &\leq \left[\sum_{i=2}^{r+1} d_i x_i\right]_p \leq \sum_{i=2}^{r+1} [x_i]_p + \frac{f(p-1)}{2} + A \\ &= \sum_{i=2}^{r+1} [x_i]_{p,f,-} + \frac{f(p-1)}{2} + A.\end{aligned}$$

In particular, for every positive integer k,

$$\left[\sum_{i=2}^{r+1} d_i \frac{p^{fk} - 1}{p^f - 1} x_i\right]_{p,fk} \leq \sum_{i=2}^{r+1} \left[\frac{p^{fk} - 1}{p^f - 1} x_i\right]_{p,fk,-} + \frac{fk(p-1)}{2} + A.$$

By Lemma 2.10, dividing by k we get

$$\left[\sum_{i=2}^{r+1} d_i x_i\right]_{p,f} \leq \sum_{i=2}^{r+1} [x_i]_{p,f,-} + \frac{f(p-1)}{2} + A/k.$$

and taking $k \to \infty$ gives us (2.9.1). The proof for case (ii) is similar.

Conversely, suppose that (2.9.1) holds for every $f \geq 1$ and every $0 \leq x_2, \dots, x_{r+1} < p^f - 1$. Let l be an integer such that $\sum_i d_i < p^l$. Then, if $0 \leq x_2, \dots, x_{r+1} < p^f - 1$, $\sum_i d_i x_i < p^{f+l} - 1$, so

$$\begin{aligned}\left[\sum_{i=2}^{r+1} d_i x_i\right]_p = \left[\sum_{i=2}^{r+1} d_i x_i\right]_{p,f+l} &\leq \sum_{i=2}^{r+1} [x_i]_{p,f+l,-} + \frac{(f+l)(p-1)}{2} \\ &= \sum_{i=2}^{r+1} [x_i]_p + \frac{f(p-1)}{2} + \frac{l(p-1)}{2},\end{aligned}$$

and (2.12.1) holds with $A = l(p-1)/2$.

Finally, suppose that (2.9.2) holds for every $f \geq 1$ and every $0 \leq x_2, \dots, x_{r+1} < p^f - 1$. Let l be an integer such that $2\sum_i d_i < p^l$. Then

$\sum_i d_i x_i + (p^{f+l}-1)/2 < p^{f+l}-1$, so

$$\begin{aligned}
1+\left[\sum_{i=2}^{r+1} d_i x_i + \frac{p^f-1}{2}\right]_p &= \left[p^{f+l} + \sum_{i=2}^{r+1} d_i x_i + \frac{p^f-1}{2}\right]_p \\
&= \left[p^f \frac{p^l+1}{2} + \sum_{i=2}^{r+1} d_i x_i + \frac{p^{f+l}-1}{2}\right]_p \\
&\le \left[\frac{p^l+1}{2}\right]_p + \left[\sum_{i=2}^{r+1} d_i x_i + \frac{p^{f+l}-1}{2}\right]_p \\
&= 1 + \frac{l(p-1)}{2} + \left[\sum_{i=2}^{r+1} d_i x_i + \frac{p^{f+l}-1}{2}\right]_{p,f+l} \\
&\le 1 + \frac{l(p-1)}{2} + \sum_{i=2}^{r+1} [x_i]_{p,f+l,-} + \frac{(f+l)(p-1)}{2} \\
&= 1 + \sum_{i=2}^{r+1} [x_i]_p + \frac{f(p-1)}{2} + l(p-1),
\end{aligned}$$

and (2.12.2) holds with $A = l(p-1)$. □

3. Theorems of finite monodromy

From known results of Kubert, explained in [Ka-RLSA, 4.1,4.2,4.3], and the result [G-K-T, Thm. 3.1], we know that G_{geom} and G_{arith} for $\mathcal{F}_{p,D,x^D,\chi_2} \otimes \alpha^{-\deg}$ are finite when q is a power of an odd prime p and D is any of

$$\frac{q+1}{2},\ \frac{q^n+1}{q+1} \text{ with odd } n,\ 2q-1.$$

We will refer to these as the known cases.

We stumbled upon the empirical fact that $\mathcal{F}_{3,23,x^{23},\chi_2} \otimes \alpha^{-\deg}$ seemed to have finite (arithmetic and geometric) monodromy, although it was not one of the known cases. As we will prove below, the monodromy is in fact finite. A computer search for each of $p = 3, 5, 7, 11$ and each $2 \le D \le 10^6$ found no other cases than this one and the known cases with finite monodromy. It is not clear whether there should be infinitely many (p, D) other that the known ones with finite monodromy, or finitely many, or just this one.

In this section, we prove that $\mathcal{F}_{3,23,x^{23},\chi_2} \otimes \alpha^{-\deg}$ has finite arithmetic and geometric monodromy groups. More generally, we prove that the two-parameter family

$$\mathcal{G}(3, 23, 1, 5, \chi_2),$$

whose traces at points $(s,t) \in \mathbb{A}^2(K)$, for $K/\mathbb{F}_3$ a finite extension, are the sums

$$(s,t) \mapsto -\sum_{x \in K^\times} \psi_K(x^{23} + sx^5 + tx)\chi_{2,K}(x)/\alpha^{-\deg(K/\mathbb{F}_3)},$$

has finite arithmetic and geometric monodromy groups. We will do so by applying the criterion from Theorem 2.12.

Theorem 3.1. *The two-parameter family*

$$\mathcal{G}(3, 23, 1, 5, \chi_2)$$

has finite arithmetic monodromy.

Proof. We will prove that for every positive integer f and every pair of integers $0 \leq x, y < 3^f$ we have the inequality

$$\left[23x + 5y + \frac{3^f - 1}{2}\right]_3 \leq [x]_3 + [y]_3 + f + 2.$$

The result follows then from Theorem 2.12.

We proceed by induction on f: for $f \leq 4$ one checks it by hand. Let $f \geq 5$ and $0 \leq x, y < 3^f$.

Case 1: $x \equiv 0 \pmod 3$.
Write $x = 3a, y = 3c + d$ with

$$a, c < 3^{f-1},\ d = 0, 1, 2.$$

Then $[5d + 1]_3 \leq [d]_3 + 1$ (check by hand), so

$$\begin{aligned}\left[23x + 5y + \frac{3^f - 1}{2}\right]_3 &= \left[3\left(23a + 5c + \frac{3^{f-1} - 1}{2}\right) + 5d + 1\right]_3 \\ &\leq \left[23a + 5c + \frac{3^{f-1} - 1}{2}\right]_3 + [5d + 1]_3 \\ &\leq [a]_3 + [c]_3 + (f + 1) + [d]_3 + 1 \\ &= [x]_3 + [y]_3 + f + 2\end{aligned}$$

by induction.

Case 2: $x \equiv 1 \pmod 3$.
Write $x = 9a + b$, $y = 9c + d$ with

$$a, c < 3^{f-2},\ b \in \{1, 4, 7\},\ d < 9.$$

Then $[23b+5d+4]_3 \le [b]_3+[d]_3+2$ (check by hand), so

$$\begin{aligned}\left[23x+5y+\frac{3^f-1}{2}\right]_3 &= \left[9\left(23a+5c+\frac{3^{f-2}-1}{2}\right)+23b+5d+4\right]_3\\ &\le \left[23a+5c+\frac{3^{f-2}-1}{2}\right]_3+[23b+5d+4]_3\\ &\le [a]_3+[c]_3+f+[b]_3+[d]_3+2\\ &= [x]_3+[y]_3+f+2\end{aligned}$$

by induction.

Case 3: $x \equiv 2 \pmod 3$ but $x \not\equiv 8, 17$ or $20 \pmod{27}$.
Write $x = 27a+b$, $y = 27c+d$ with

$$a, c < 3^{f-3},\ b \in \{2,5,11,14,23,26\},\ d < 27.$$

Then $[23b+5d+13]_3 \le [b]_3+[d]_3+3$ (check by hand), so

$$\begin{aligned}\left[23x+5y+\frac{3^f-1}{2}\right]_3 &= \left[27\left(23a+5c+\frac{3^{f-3}-1}{2}\right)+23b+5d+13\right]_3\\ &\le \left[23a+5c+\frac{3^{f-3}-1}{2}\right]_3+[23b+5d+13]_3\\ &\le [a]_3+[c]_3+(f-1)+[b]_3+[d]_3+3\\ &= [x]_3+[y]_3+f+2\end{aligned}$$

by induction.

Case 4: $x \equiv 8, 17$ or $20 \pmod{27}$.
Write $x = 81a+b$, $y = 81c+d$ with

$$a, c < 3^{f-4},\ b \in \{8,17,20,35,44,47,62,71,74\},\ d < 81.$$

Then $[23b+5d+40]_3 \le [b]_3+[d]_3+4$ (check by hand), so

$$\begin{aligned}\left[23x+5y+\frac{3^f-1}{2}\right]_3 &= \left[81\left(23a+5c+\frac{3^{f-4}-1}{2}\right)+23b+5d+40\right]_3\\ &\le \left[23a+5c+\frac{3^{f-4}-1}{2}\right]_3+[23b+5d+40]_3\\ &\le [a]_3+[c]_3+(f-2)+[b]_3+[d]_3+4\\ &= [x]_3+[y]_3+f+2\end{aligned}$$

by induction. □

4. Determination of the monodromy groups

In this section, we will show that with the correct choice [Ka-NG2, 1.7] of α, namely

$$\alpha := -g(\psi, \chi_2),$$

with $g(\psi, \chi_2)$ the quadratic Gauss sum over $\mathbb{F}_3$, we can determine the monodromy of $\mathcal{F}_{3,23,x^{23},\chi_2} \otimes \alpha^{-\deg}$, and of some other related local systems, exactly. Recall from Lemma 2.3 that we have

$$G_{geom} \lhd G_{arith} < \mathrm{SO}_{23}(\overline{\mathbb{Q}_\ell}).$$

Thus G_{geom} is an irreducible, primitive (by Lemma 1.1) finite subgroup of $\mathrm{SO}_{23}(\overline{\mathbb{Q}_\ell})$. The larger group G_{arith} is a fortiori also an irreducible, primitive finite subgroup of $\mathrm{SO}_{23}(\overline{\mathbb{Q}_\ell})$.

The traces attained by $\mathcal{F}_{3,23,x^{23},\chi_2} \otimes \alpha^{-\deg}$, i.e, the traces of elements of G_{arith}, are all integers (being algebraic integers in $\mathbb{Q}(\zeta_3)^+ = \mathbb{Q}$). Over the field $\mathbb{F}_{81}$, the traces obtained are, by direct calculation, $\{-2, -1, 0, 1, 2, 3\}$. Over $\mathbb{F}_{243}$, the traces attained are, by direct calculation, $\{-5, -2, -1, 0, 1, 2\}$.

Finally, we recall that from Lemma 1.2 that the image of the wild inertia group is the additive group of $\mathbb{F}_{3^5}$, the least extension of $\mathbb{F}_3$ containing the 22'nd roots of unity.

First we prove the following theorem on finite subgroups of $\mathrm{SL}_{23}(\mathbb{C})$:

Theorem 4.1. *Let $V = \mathbb{C}^{23}$ and let $G < \mathrm{SL}(V)$ be a finite irreducible subgroup. Let χ denote the character of G afforded by V, and suppose that all the following conditions hold:*

(i) *χ is real-valued;*
(ii) *χ is primitive;*
(iii) *$\chi(g) < -1$ for some $g \in G$;*
(iv) *The 3-rank of G is at least 5.*

Then $G \cong \mathsf{Co}_3$ in its unique (orthogonal) irreducible representation of degree 23.

Proof. By the assumption, the G-module V is irreducible and primitive; furthermore, it is tensor indecomposable and not tensor induced since $\dim V = 23$ is prime. Next, we observe by Schur's Lemma that condition (i) implies $\mathbf{Z}(G) = 1$. Now we can apply [G-T, Proposition 2.8] (noting that the subgroup H in its proof is just G since $G < \mathrm{SL}(V)$) and arrive at one of the following two cases.

(a) *Extraspecial case*: $P \lhd G$ for some extraspecial 23-group of order 23^3 that acts irreducibly on V. But in this case, $\chi|_P$ cannot be real-valued (in fact, $\mathbb{Q}(\chi|_P)$ would be $\mathbb{Q}(\exp(2\pi i/23))$, violating (i).

(b) *Almost simple case*: $S \lhd G \leq \mathrm{Aut}(S)$ for some finite non-abelian simple group S. In this case, we can apply the main result of [H-M] and arrive at one of the following possibilities for S.

• $S = \mathsf{A}_{24}$, M_{24}, or $\mathrm{PSL}_2(23)$. Correspondingly, we have that $G = \mathsf{A}_{24}$ or S_{24}, M_{24}, and $\mathrm{PSL}_2(23)$ or $\mathrm{PGL}_2(23)$. In all of these possibilities, $\chi(x) \geq -1$ for $x \in G$ by [ATLAS], violating (iii).

• $S = \mathrm{PSL}_2(47)$. This is ruled out since $\mathbb{Q}(\chi|_S)$ would be $\mathbb{Q}(\sqrt{-47})$, violating (i).

• $S = \mathsf{Co}_2$. In this case, $G = S$, and a Sylow 3-subgroup P of G has a normal extraspecial 3-subgroup $Q \cong 3_+^{1+4}$ of index 3, see [ATLAS]. Since G has 3-rank ≥ 5 by (iv), P contains an elementary abelian 3-subgroup of order 3^5, whence Q contains a subgroup $R \cong C_3^4$. Identifying $\mathbf{Z}(Q)$ with $\mathbb{F}_3$, we see that the commutator map induces a non-degenerate symplectic form on $Q/\mathbf{Z}(Q) \cong \mathbb{F}_3^4$. As R is abelian, this form is totally isotropic on $\mathbf{Z}(Q)R/\mathbf{Z}(Q)$ which has order at least 3^3. But this is a contradiction, since any isotropic subspace in $\mathbb{F}_3^4$ has dimension at most 2.

• $S = \mathsf{Co}_3$. In this case $G = \mathsf{Co}_3$, as stated. □

Theorem 4.2. *We have the following results.*

(i) *For $\mathcal{F}_{3,23,x^{23},\chi_2} \otimes \alpha^{-\deg}$, we have $G_{geom} = G_{arith} = \mathsf{Co}_3$, the Conway group Co_3, in its irreducible orthogonal representation of dimension 23.*

(ii) *For the two-parameter family $\mathcal{G}(3, 23, 1, 5, \chi_2)$, we have $G_{geom} = G_{arith} = \mathsf{Co}_3$.*

(iii) *The local system on $\mathbb{G}_m \times \mathbb{A}^2/\mathbb{F}_3$ whose trace is given as follows: for any finite extension $K/\mathbb{F}_3$, and any $(r \neq 0, s, t) \in \mathbb{G}_m(K) \times \mathbb{A}^2(K)$,*

$$(r, s, t) \mapsto -\chi_{2,K}(r) \sum_{x \in K^\times} \psi_K(rx^{23} + sx^5 + tx)\chi_{2,K}(x)/\alpha^{-\deg(K/\mathbb{F}_p)},$$

has $G_{geom} = G_{arith} = \mathsf{Co}_3$.

(iv) *For any finite extension $K/\mathbb{F}_3$, and any $s_0 \in K$, the local system on $\mathbb{A}^1/K$ whose trace function, at points $t \in L$, L a finite extension of K, is given by*

$$t \mapsto -\sum_{x \in L^\times} \psi_L(x^{23} + s_0 x^5 + tx)\chi_{2,L}(x)/\alpha^{-\deg(L/\mathbb{F}_p)},$$

has $G_{geom} = G_{arith} = \mathsf{Co}_3$.

(v) *The local system on* $\mathbb{A}^1/\mathbb{F}_3$ *whose trace function, at points* $t \in K$, K *a finite extension of* $\mathbb{F}_3$, *is given by*

$$t \mapsto -\sum_{x \in K^\times} \psi_L(x^{23} + tx^5)\chi_{2,K}(x)/\alpha^{-\deg(K/\mathbb{F}_p)},$$

has $G_{geom} = G_{arith} = \mathsf{Co}_3$.

(vi) *For any finite extension* K *of* $\mathbb{F}_3$, *and any* $(s_0, t_0) \in \mathbb{A}^2(K)$ *other than* $(0,0)$, *the local system on* $\mathbb{G}_m/K$ *whose trace function at points* $r \in L^\times$, L *a finite extension of* K, *is given by*

$$r \mapsto -\chi_{2,L}(r)\sum_{x \in L^\times} \psi_L(rx^{23} + s_0x^5 + t_0x)\chi_{2,L}(x)/\alpha^{-\deg(L/\mathbb{F}_p)},$$

has $G_{geom} = G_{arith} = \mathsf{Co}_3$.

Proof. We first note that among finite irreducible subgroups of $\mathrm{SO}_{23}(\mathbb{C})$, the Conway group Co_3 is both maximal **and** minimal. Indeed, the minimality is clear from the [ATLAS] list of maximal subgroups of Co_3 and their character tables. The maximality is clear from Theorem 4.1.

The local system in (iv) has finite monodromy because its restriction to the dense open set $(\mathbb{G}_m)^3/\mathbb{F}_3$ has finite monodromy, being the $\mathcal{G}_{big}$ partner, in the sense of Lemma 2.6 of two-parameter local system of (ii). The $\chi_2(t)$ term in front keeps its G_{arith} in $\mathrm{SO}_{23}(\mathbb{C})$, by [Ka-NG2, 1.7]. It is geometrically irreducible because this is so already after pullback to the $(1,0,t)$ t-line, where it is $\mathcal{F}_{3,23,x^{23},\chi_2} \otimes \alpha^{-\deg}$.

We remark that the local system in (v) is geometrically irreducible, because it is the Fourier Transform of $[5]_\star(\mathcal{L}_{\psi(x^{23})} \otimes \mathcal{L}_{\chi_2(x)})$, a middle extension sheaf (cf. [Ka-TLFM, proof of 3.3.1]) which is geometrically irreducible. Indeed it is $I(\infty)$-irreducible, because its five $I(\infty)$-slopes are each $23/5$, with exact denominator 5.

We also remark that the local system in (vi) is geometrically irreducible, because it is $\mathcal{L}_{\chi_2(t)}$ tensored with the Fourier Transform of $[23]_\star(\mathcal{L}_{\psi(s_0x^5+r_0x)} \otimes \mathcal{L}_{\chi_2(x)})$, a middle extension sheaf (cf. [Ka-TLFM, proof of 3.3.1]) which is geometrically irreducible. Indeed it is $I(\infty)$-irreducible, because its 23 $I(\infty)$-slopes are each either $5/23$, with exact denominator 23, if $s_0 \neq 0$, or each $1/23$ if $s_0 = 0$ but $r_0 \neq 0$.

Thus it suffices to prove (i). For then (ii) and (iii) follows from (i) and the maximality of Co_3 as a finite irreducible subgroup of $\mathrm{SO}_{23}(\mathbb{C})$, and then (iv), (v) and (vi) each follow from (ii) and (iii) and the minimality of Co_3 as a finite irreducible subgroup of $\mathrm{SO}_{23}(\mathbb{C})$.

For case (i), we apply Theorem 4.1 to G_{arith}, to conclude that $G_{arith} = \mathsf{Co}_3$. Then we use minimality of Co_3 to conclude that $G_{geom} = \mathsf{Co}_3$. □

References

[ATLAS] Conway, J. H., Curtis, R. T., Norton, S. P., Parker, R. A. and Wilson, R. A., Atlas of finite groups. Maximal subgroups and ordinary characters for simple groups. With computational assistance from J. G. Thackray. Oxford University Press, Eynsham, 1985.

[De-Weil II] Deligne, P., La conjecture de Weil II, Publ. Math. IHES **52** (1981), 313–428.

[G-K-T] Guralnick, R. M., Katz, N., and Tiep, P. H., Rigid local systems and alternating groups, Tunis. J. Math. **1** (2019), 295–320.

[G-T] Guralnick, R. M. and Tiep, P. H., Symmetric powers and a conjecture of Kollar and Larsen, Invent. Math. **174** (2008), 505–554.

[H-M] Hiss, G. and Malle, G., Low-dimensional representations of quasi-simple groups, LMS J. Comput. Math. **4** (2001), 22–63.

[Ka-ESDE] Katz, N., Exponential sums and differential equations. Annals of Mathematics Studies, 124. Princeton Univ. Press, Princeton, NJ, 1990. xii+430 pp.

[Ka-NG2] Katz, N., Notes on G_2, determinants, and equidistribution, Finite Flelds Appl. **10** (2004), 221–269.

[Ka-RL] Katz, N., and Rojas-León, A., Rigid local systems with monodromy group $2.J_2$, Finite Fields Appl. **57** (2019), 276–286.

[Ka-RLSA] Katz, N., Rigid local systems on $\mathbb{A}^1$ with finite monodromy, Mathematika **64** (2018), 785–846.

[Ka-TLFM] Twisted L-functions and monodromy. Annals of Mathematics Studies, 150. Princeton University Press, Princeton, NJ, 2002. viii+249 pp.

[Lau] Laumon, G., Transformation de Fourier, constantes d'équations fonctionnelles et conjecture de Weil, Publ. Math. IHES **65** (1987) 131–210.

[R-L] Rojas-León, A., Finite monodromy of some families of exponential sums, J. Number Theory **197** (2019), 37–48.

[Such] Šuch, Ondrej, Monodromy of Airy and Kloosterman sheaves, Duke Math. J. **103** (2000), 397–444.

Department of Mathematics, Princeton University, Princeton, NJ 08544, USA

E-mail address: nmk@math.princeton.edu

Departamento de Álgebra, Universidad de Sevilla, c/Tarfia s/n, 41012 Sevilla, Spain

E-mail address: arojas@us.es

Department of Mathematics, Rutgers University, Piscataway, NJ 08854, USA

E-mail address: tiep@math.rutgers.edu