TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 00, Number 0, Pages 000–000
S 0002-9947(XX)0000-0

A RIGID LOCAL SYSTEM WITH MONODROMY GROUP THE BIG CONWAY GROUP $2.\mathsf{Co}_1$ AND TWO OTHERS WITH MONODROMY GROUP THE SUZUKI GROUP $6.\mathsf{Suz}$

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

ABSTRACT. We first develop some basic facts about hypergeometric sheaves on the multiplicative group $\mathbb{G}_m$ in characteristic $p > 0$. Specializing to some special classes of hypergeometric sheaves, we give relatively "simple" formulas for their trace functions, and a criterion for them to have finite monodromy. We then show that one of our local systems, of rank 24 in characteristic $p = 2$, has the big Conway group $2.\mathsf{Co}_1$, in its irreducible orthogonal representation of degree 24 as the automorphism group of the Leech lattice, as its arithmetic and geometric monodromy groups. Each of the other two, of rank 12 in characteristic $p = 3$, has the Suzuki group $6.\mathsf{Suz}$, in one of its irreducible representations of degree 12 as the $\mathbb{Q}(\zeta_3)$-automorphisms of the Leech lattice, as its arithmetic and geometric monodromy groups. We also show that the pullback of these local systems by $x \mapsto x^N$ maps to the affine line $\mathbb{A}^1$ yields the same arithmetic and geometric monodromy groups.

CONTENTS

INTRODUCTION

In the first three sections, we develop some basic facts about hypergeometric sheaves on the multiplicative group $\mathbb{G}_m$ in characteristic $p > 0$. In the fourth and fifth sections, we specialize to quite special classes of hypergeometric sheaves. We give relatively "simple" formulas for their trace functions, and a criterion for

2010 *Mathematics Subject Classification.* Primary 11T23, Secondary 20C15, 20C34, 20D08.
Key words and phrases. Rigid local systems, Monodromy groups, Sporadic simple groups.
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) and the Joshua Barlaz Chair in Mathematics.
The authors are grateful to the referee for careful reading and helpful comments on the paper.

them to have finite monodromy. In the next section, we prove that three of them have finite monodromy groups. We then give some results on finite complex linear groups. We next use these group theoretic results to show that one of our local systems, of rank 24 in characteristic $p = 2$, has the big Conway group $2.\mathsf{Co}_1$, in its irreducible orthogonal representation of degree 24 as the automorphism group of the Leech lattice, as its arithmetic and geometric monodromy groups. Each of the other two, of rank 12 in characteristic $p = 3$, has the Suzuki group $6.\mathsf{Suz}$, in one of its irreducible representations of degree 12 as the $\mathbb{Q}(\zeta_3)$-automorphisms of the Leech lattice, as its arithmetic and geometric monodromy groups. In the final section, we pull back these local systems by $x \mapsto x^N$ maps to the affine line $\mathbb{A}^1$, and show that after pullback their arithmetic and geometric monodromy groups remain the same. Sadly the Leech lattice makes no appearance in our arguments.

This paper is part of a program to exhibit simple (in the sense of "simple to remember") Kloosterman and hypergeometric sheaves whose monodromy groups are "interesting" finite groups, cf. our earlier papers [Ka-RL], [Ka-RL-T-Co2], and [Ka-RL-T-Co3]. The reader may wonder if we could hope to obtain in this way, for instance, the Monster – the largest sporadic simple group. The answer is sadly no, for the following reason. In a Kloosterman or hypergeometric sheaf, its monodromy group cannot possibly be finite unless its local monodromies at both 0 and ∞ are finite. One knows that this finiteness of local monodromy forces the "upstairs" characters (and the "downstairs" characters, if any) of the sheaf to be pairwise distinct. This pairwise distinctness severely limits the list of finite, in particular almost quasisimple, groups that we could hope to attain, and rules out the Monster. See the forthcoming paper [Ka-T] for a detailed discussion of this and related topics.

1. Primitivity

We consider, in characteristic $p > 0$, a $\overline{\mathbb{Q}}_\ell$ $(\ell \neq p)$ -hypergeometric sheaf $\mathcal{H}$ of type (n, m), with $n > m > 0$, thus

$$\mathcal{H} = \mathcal{H}yp(\psi, \chi_1, \ldots, \chi_n; \rho_1, \ldots, \rho_m).$$

Here ψ is a nontrivial additive character of some finite extension $\mathbb{F}_q/\mathbb{F}_p$, and the χ_i and ρ_j are (possibly trivial) multiplicative characters of $\mathbb{F}_q^\times$, with the proviso that no χ_i is any ρ_j. One knows [Ka-ESDE, 8.4.2, (1)] that such an $\mathcal{H}$ is lisse on $\mathbb{G}_m$, geometrically irreducible, and on $\mathbb{G}_m/\overline{\mathbb{F}_q}$ has Euler characteristic -1. Its local monodromy at 0 is of finite order if and only if the χ_i are pairwise distinct, in which case the image of the inertia group $I(0)$ acts on the sheaf via the direct sum $\oplus_i \chi_i$, cf. [Ka-ESDE, 8.4.2, (5)]. Its local monodromy at ∞ is of finite order if and only the ρ_j are pairwise distinct, in which case the image of the inertia group $I(\infty)$ acts on the sheaf via the direct sum of $\oplus_j \rho_j$ with a totally wild representation Wild_{n-m} of rank $n - m$ and Swan conductor one, i.e. it has all ∞-breaks $1/(n - m)$. The necessity results from the fact that any repetition of the ρ_j produces nontrivial Jordan blocks. The sufficiency is given by the following lemma.

Lemma 1.1. *If the ρ_j are pairwise distinct, then the $I(\infty)$-action on $\mathcal{H}$ factors through a finite quotient of $I(\infty)$.*

Proof. The $I(\infty)$-representation is the direct sum of the $n - m$ Kummer sheaves $\mathcal{L}_\rho$, together with a wild part Wild_{n-m} of rank $n - m$ and Swan conductor one, with all breaks $1/(n - m)$. This wild part Wild_{n-m} is $I(\infty)$-irreducible (because all its slopes are $1/(n - m)$). The action of $I(\infty)$ is thus completely reducible. Because this action is the restriction of an action of the decomposition group $D(\infty)$, the local monodromy theorem assures us that on an open normal subgroup of $I(\infty)$, the representation becomes unipotent. But it remains completely reducible, so it becomes trivial. $\square$

Proposition 1.2. *Suppose that $\mathcal{H}$ is geometrically induced, i.e. that there exists a smooth connected curve $U/\overline{\mathbb{F}_q}$, a finite étale map $\pi : U \to \mathbb{G}_m/\overline{\mathbb{F}_q}$ of degree $d \geq 2$, a lisse sheaf $\mathcal{G}$ on U, and an isomorphism $\mathcal{H} \cong \pi_\star\mathcal{G}$. Then up to isomorphism we are in one of the following situations.*

(i) (**Kummer induced**) *$U = \mathbb{G}_m$, π is the N^{th} power map $x \mapsto x^N$ for some $N \geq 2$ prime to p with $N|n$ and $N|m$, $\mathcal{G}$ is a hypergeometric sheaf of type $(n/N, m/N)$, and the lists of χ_i and of ρ_j are each stable under multiplication by any chararacter Λ of order dividing N.*

(ii) (**Belyi induced**) *$U = \mathbb{G}_m \setminus \{1\}$, π is either $x \mapsto x^A(1-x)^B$ or is $x \mapsto x^{-A}(1-x)^{-B}$, $\mathcal{G}$ is $\mathcal{L}_{\Lambda(x)} \otimes \mathcal{L}_{\sigma(x-1)}$ for some multiplicative characters Λ and σ, and one of the following holds:*
  (a) *Both A, B are prime to p, but $A+B = d_0p^r$ with $p \nmid d_0$ and $r \geq 1$. In this case π is $x \mapsto x^A(1-x)^B$, the χ_i are all the A^{th} roots of Λ and all B^{th} roots of σ, and the ρ_j are all the ${d_0}^{\text{th}}$ roots of $(\Lambda\sigma)^{1/p^r}$.*
  (b) *A is prime to p, $B = d_0p^r$ with $p \nmid d_0$ and $r \geq 1$. In this case π is $x \mapsto x^{-A}(1-x)^{-B}$, the χ_i are all the $(A+B)^{\text{th}}$ roots of $\Lambda\sigma$, and the ρ_j are all the A^{th} roots of Λ and all the ${d_0}^{\text{th}}$ roots of σ^{1/p^r}.*
  (c) *B is prime to p, $A = d_0p^r$ with $p \nmid d_0$ and $r \geq 1$. In this case π is $x \mapsto x^{-A}(1-x)^{-B}$, the χ_i are all the $(A+B)^{\text{th}}$ roots of $\Lambda\sigma$, and the ρ_j are all the B^{th} roots of σ together with all the ${d_0}^{\text{th}}$ roots of Λ^{1/p^r}.*

Proof. If $\mathcal{H}$ is $\pi_\star\mathcal{G}$, then we have the equality of Euler Poincaré characteristics

$$\mathsf{EP}(U, \mathcal{G}) = \mathsf{EP}(\mathbb{G}_m/\overline{\mathbb{F}_p}, \pi_\star\mathcal{G}) = \mathsf{EP}(\mathbb{G}_m/\overline{\mathbb{F}_p}, \mathcal{H}) = -1.$$

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

$$\begin{aligned} -1 = \mathsf{EP}(U, \mathcal{G}) &= \mathrm{rank}(\mathcal{G})(2 - 2g_X - \#(\pi^{-1}(0)) - \#(\pi^{-1}(\infty))) \\ &- \sum_{w \in \pi^{-1}(0)} \mathsf{Swan}_w(\mathcal{G}) - \sum_{w \in \pi^{-1}(\infty)} \mathsf{Swan}_w(\mathcal{G}). \end{aligned}$$

This shows that $g_X = 0$, otherwise the coefficient of $\mathrm{rank}(\mathcal{G})$ is too negative. Then the sum

$$\#(\pi^{-1}(0)) + \#(\pi^{-1}(\infty)) \leq 3,$$

for the same reason. As each summand is strictly positive, we have one of two cases. Case (i) is

$$\#(\pi^{-1}(0)) = \#(\pi^{-1}(\infty)) = 1.$$

On the source $X = \mathbb{P}^1$, we may assume $\pi^{-1}(0) = 0$ and $\pi^{-1}(\infty) = \infty$.

Case (ii) is that, after possibly interchanging 0 and ∞ on the target $\mathbb{G}_m$ by $x \mapsto 1/x$, we have

$$\#(\pi^{-1}(0)) = 2, \ \#(\pi^{-1}(\infty)) = 1.$$

On the source $X = \mathbb{P}^1$, we may assume $\pi^{-1}(0) = \{0, 1\}$ and $\pi^{-1}(\infty) = \infty$. We then have that $\mathcal{G}$ is lisse of rank one on $\mathbb{P}^1 \setminus \{0, 1, \infty\}$, and everywhere tame, so it is $\mathcal{L}_{\Lambda(x)} \otimes \mathcal{L}_{\sigma(x-1)}$ for some multiplicative characters Λ and σ,

We first treat case (i). Here π is a finite étale map from $\mathbb{G}_m/\overline{\mathbb{F}_q}$ to itself of degree ≥ 2, which sends 0 to itself and ∞ to itself, so necessarily (a nonzero constant multiple of) the N^{th} power map, for some $N \geq 2$ prime to p. In this case the Euler-Poincaré formula shows that

$$\mathsf{Swan}_0(\mathcal{G}) + \mathsf{Swan}_\infty(\mathcal{G}) = 1.$$

The lisse sheaf $\mathcal{G}$ is geometrically irreducible (because its direct image $\pi_\star\mathcal{G} \cong \mathcal{H}$ is). Therefore [Ka-ESDE, 8.5.3.1] $\mathcal{G}$ is itself a hypergeometric sheaf, and $[N]_\star\mathcal{G} \cong \mathcal{H}$. In this case of Kummer induction, the rest follows from [Ka-ESDE, 8.9.1 and 8.9.2].

We now turn to case (ii). The map $\pi : \mathbb{A}^1 \setminus \{0, 1\} \to \mathbb{G}_m$ is given by (a nonzero constant multiple of) a polynomial $\pi(x) = f(x) = x^A(1-x)^B$ for some integers $A, B \geq 0$. This map being finite étale insures that at least one of A or B is prime to p (otherwise $f(x)$ is a p^{th} power). If either A or B vanishes, then possibly after $x \mapsto 1-x$ we have $B = 0$, and we are in case (1), with $N = A$. Thus both A and B are strictly positive integers, at least one of which is prime to p.

The polynomial $f(x) = x^A(1-x)^B$ defines a finite étale map from $\mathbb{A}^1 \setminus \{0, 1\}$ to $\mathbb{G}_m$ if and only if the derivative $f'(x)$ has all its zeroes in the set $\{0, 1\}$. Let us say that a zero outside $\{0, 1\}$ is a "bad" zero. We readily calculate

$$f'(x) = \left(\frac{A}{x} + \frac{-B}{1-x}\right) f(x) = \left(\frac{A - (A+B)x}{x(1-x)}\right) f(x).$$

If $A+B$ is 0 mod p, there are no bad zeroes. This will be subcase (a). If $A+B$ nonzero mod p, then there is a zero at $x = A/(A+B)$. For this not to be a bad zero, either A must be 0 mod p, or A must be $A+B$ mod p, i.e., either A or B must be 0 mod p. These are subcases (b) and (c).

In subcase (a), we readliy compute the tame characters occurring in local monodromies at 0 and at ∞ of $\pi_\star\mathcal{G}$, with $\mathcal{G} = \mathcal{L}_{\Lambda(x)} \otimes \mathcal{L}_{\sigma(x-1)}$. In subcases (b) and (c), we do the same, now using $\pi(x) := \frac{1}{x^A(1-x)^B}$. We know that $\pi_\star\mathcal{G}$ has Euler Poincaré characteristic -1. If there are no tame characters that occur both at 0 and at ∞, this data determines [Ka-ESDE, 8.5.6], up to multiplicative translation, the geometrically irreducible hypergeometric sheaf which is the direct image. [If there are tame characters in common, this direct image is geometrically reducible [Ka-ESDE, 8.4.7]. Being semisimple, it is the sum of Kummer sheaves $\mathcal{L}_\chi$ for each χ in common, and a geometrically irreducible hypergeometric sheaf of lower rank.] $\square$

Corollary 1.3. *If an irreducible hypergeometric sheaf $\mathcal{H}$ of type $(n, 1)$ with $n \geq 2$ is geometrically induced, then its rank is a power of p.*

Proof. It cannot be Kummer induced of degree $N \geq 2$, because N must divide $\gcd(n, 1)$. In case (2), subcases (b) and (c), there are at least two tame characters at ∞. In subcase (a), there is just one tame character at ∞ precisely when $A + B = n$ is a power of p (i.e., when $d_0 = 1$ in that subcase). $\square$

Corollary 1.4. *An irreducible hypergeometric sheaf $\mathcal{H}$ of type (n, m) with $n > m > 1$ and n a power of p is not geometrically induced.*

Proof. It cannot be Kummer induced of degree $d \geq 2$, because d is prime to p but divides the rank n of $\mathcal{H}$. In case (ii), we must be in subcase (a), otherwise the rank is prime to p. In subcase (a), there is just one tame character at ∞, because $d_0 = 1$ in that subcase. $\square$

Remark 1.5. Suppose that N is prime to p. As Sawin has pointed out to us, for $\pi(x) = \frac{1}{x^{Nq}(1-x)}$, $\pi_\star\mathbb{1}$ is the direct sum of $\mathbb{1}$ with

$$\mathcal{H}yp(\psi, \text{all } \chi \text{ nontrivial with } \chi^{Nq+1} = \mathbb{1}; \text{all } \rho \text{ with } \rho^N = \mathbb{1}).$$

This last sheaf is thus "almost" induced from rank one, and hence has finite geometric monodromy. In particular, for $N = 1$,

$$\mathcal{H}yp(\psi, \text{ all } \chi \text{ nontrivial with } \chi^{q+1} = \mathbb{1}; \mathbb{1})$$

is "almost" induced and has finite geometric monodromy.

Similarly, for $\pi(x) = x^{Nq-1}(1-x)$, $\pi_\star\mathbb{1}$ is the direct sum of $\mathbb{1}$ with

$$\mathcal{H}yp(\psi, \text{all } \chi \text{ with } \chi^{Nq-1} = \mathbb{1}; \text{all nontrivial } \rho \text{ with } \rho^N = \mathbb{1}).$$

This last sheaf is thus "almost" induced from rank one, and hence has finite geometric monodromy. The particular case $N = 2$ is the one treated in [G-K-T].

2. Tensor indecomposability

Over a field k, a representation $\Phi : G \to \mathrm{GL}(V)$ of a group G is called *tensor decomposable* if there exists a k-linear isomorphism $V \cong A \otimes_k B$ with both A, B of dimension ≥ 2, such that $\Phi(G) \leq \mathrm{GL}(A) \otimes_k \mathrm{GL}(B)$, the latter being the image of $\mathrm{GL}(A) \times \mathrm{GL}(B)$ in $\mathrm{GL}(A \otimes_k B)$ by the map $(\phi, \rho) \mapsto \phi \otimes \rho$.

In this situation, it is well known (also see the proof of Theorem 2.4 for more detail) that both A and B can be given the structure of projective representations of G, in such a way that the k-linear isomorphism $V \cong A \otimes_k B$ becomes an isomorphism of projective representations.

In reading the literature, it is important to distinguish this notion from the stronger notion of *linearly tensor decomposable* that both A and B are kG-modules such that the k-linear isomorphism $V \cong A \otimes_k B$ becomes an isomorphism of kG-modules.

We use the term *tensor indecomposable* to mean "not tensor decomposable" (and so "tensor indecomposable" is stronger than "linearly tensor indecomposable", cf. Remark 2.5).

The target of this section is the following theorem.

Theorem 2.1. *In characteristic $p > 0$ and with $\ell \neq p$, a $\overline{\mathbb{Q}_\ell}$-hypergeometric sheaf*

$$\mathcal{H} = \mathcal{H}yp(\psi, \chi_1, \ldots, \chi_n; \rho_1, \ldots, \rho_m).$$

of the type in Lemma 1.1, i.e. one of type $n > m > 0$ with the "downstairs" characters ρ_i pairwise distinct, is tensor indecomposable as a representation of $\pi_1(\mathbb{G}_m/\overline{\mathbb{F}_p})$ if either of the following conditions holds:

(i) $n \neq 4$.
(ii) $n = 4$, $p = 2$, *and* $m > 1$.
(iii) $n = 4$, $p > 2$, *and* $m \neq 2$.

Remark 2.2. In order to show that a representation of a group G is tensor indecomposable, it suffices to exhibit a subgroup H of G such that the restriction to H of the representation is tensor indecomposable as a representation of H. We will do this by taking the subgroup $I(\infty)$. In view of Lemma 1.1, $I(\infty)$ acts through a finite quotient group. In Theorem 2.4 below, we argue directly with this finite quotient group. In the Appendix, we give another approach to this same result. There we again use Lemma 1.1, this time combined with the fact that $I(\infty)$ has cohomological dimension ≤ 1 (in the suitable profinite world) to show first that if the representation is tensor decomposable then in fact it is linearly tensor decomposable, and then we show that this is impossible under either of the stated hypotheses.

We will need the following consequence of the main results of [BNRT], which in turn rely on [GT1] and [M]:

Theorem 2.3. *Let α be a complex irreducible character of a finite solvable group G, of degree $\alpha(1) = d \geq 3$. Assume in addition that G has abelian Sylow 2-subgroups if $2 \nmid d$. Then α has 4^{th} moment at least 3, equivalently, $\alpha\overline{\alpha} - 1_G$ is not irreducible.*

Proof. Without loss we may assume that α is faithful, and let α be afforded by a complex irreducible G-module $W = \mathbb{C}^d$. Then we can apply the main results of [BNRT] to the subgroup $G < \mathcal{G} := \mathrm{GL}(W)$.

First consider the case $d \geq 5$. By [BNRT, Theorem 3] and using the solvability of G, we see that we must be in the extraspecial case; in particular, $d = p^n$ is a power of some prime p and G has a quotient H which is a subgroup of $\mathrm{Sp}_{2n}(p)$ that satisfies the conclusions if [BNRT, Theorem 5]. Since H is solvable, we arrive at one of the following possibilities.

(i) $p^n = 5$, $H = \mathrm{SL}_2(3)$.
(ii) $p^n = 7$, $H = \mathrm{SL}_2(3) \rtimes C_2$.
(iii) $p^n = 9$, $H =$ `SmallGroup`$(160, 199)$, `SmallGroup`$(320, 1581)$, in the notation of [GAP] (and one can check that a Sylow 2-subgroup of H has an irreducible character of degree 4).

In all these cases, $2 \nmid d$, but H has non-abelian Sylow 2-subgroups, contrary to our assumption.

Next let $d = 3$. Since G is solvable, by [BNRT, Theorem 10(B)], we have that $\mathbf{Z}(\mathcal{G})G = \mathbf{Z}(\mathcal{G})H$, where H is a finite group whose Sylow 2-subgroups are quaternion of order 8. It follows that Sylow 2-subgroups of G are not abelian, again contradicting our assumption.

Finally, let $d = 4$. Applying [BNRT, Theorem 8(A)], we see that G always admits A_5 as a subquotient, and so it is not solvable. $\square$

We begin with the fraction field K of a henselian discrete valuation ring R whose residue field k is algebraically closed of characteristic $p > 0$, and consider a separable closure K^{sep} of K. Then we have $I := \mathrm{Gal}(K^{sep}/K)$ the inertia group, and $P \lhd I$ the p-Sylow subgroup of I. We fix a prime $\ell \neq p$, an algebraic closure $\overline{\mathbb{Q}}_\ell$ of $\mathbb{Q}_\ell$, and work in the category of continuous, finite dimensional $\overline{\mathbb{Q}}_\ell$-representations of I (which we will call simply "representations of I"). Note that any finite quotient group J of I is a finite group, with normal Sylow p-subgroup (which we will also denote by P) and with cyclic quotient J/P.

Theorem 2.4. *Let J be a finite group, with normal Sylow p-subgroup P and with cyclic quotient J/P. Let V be a finite-dimensional $\mathbb{C}J$-module which is the direct sum $T \oplus W$ of a nonzero tame part T (i.e., one on which P acts trivially) and of an irreducible submodule W which is totally wild (i.e., one in which P has no nonzero invariants). Suppose that one of the following conditions holds.*

(a) $\dim(V) \neq 4$.
(b) $\dim(V) = 4$, $p = 2$, *and* $\dim(T) > 1$.

(c) $\dim(V) = 4$, $p > 2$, *and* $\dim(T) \neq 2$.

Then J does not stabilize any decomposition $V = A \otimes B$ with $\dim(A), \dim(B) > 1$.

Proof. (i) Suppose that J fixes a decomposition $V = A \otimes B$ with $\dim(A), \dim(B) > 1$. Fix a basis $(e_1, \ldots, e_k)$ of A and a basis $(f_1, \ldots, f_l)$ of B, so that $(e_i \otimes f_j \mid 1 \leq i \leq k, 1 \leq j \leq l)$ is a basis of V. Let $\Phi : J \to \mathrm{GL}_{\dim(V)}(\mathbb{C})$ denote the matrix representation of J on V with respect to this basis. Then for each $g \in J$, we can find matrices $\Theta(g) \in \mathrm{GL}_{\dim(A)}(\mathbb{C})$ and $\Psi(g) \in \mathrm{GL}_{\dim(B)}(\mathbb{C})$ such that

$$\Phi(g) = \Theta(g) \otimes \Psi(g). \tag{2.4.1}$$

Note that if X and Y are invertible matrices (of possibly different sizes) over any field $\mathbb{F}$ so that $X \otimes Y$ is the identity matrix, then X and Y are scalar matrices (of the corresponding sizes), inverses to each other. It follows that if $X \otimes Y = X' \otimes Y'$ for some invertible matrices X, X' of the same size and invertible matrices Y, Y' of the same size, then $X' = \gamma X$ and $Y' = \gamma^{-1} Y$ for some $\gamma \in \mathbb{F}^\times$.

Now, for any $g, h \in J$, by (2.4.1) we have

$$\Theta(g)\Theta(h) \otimes \Psi(g)\Psi(h) = (\Theta(g) \otimes \Psi(g))(\Theta(h) \otimes \Psi(h)) = \Phi(g)\Phi(h) = \Phi(gh) = \Theta(gh) \otimes \Psi(gh).$$

By the above observation, $\Theta(gh) = \gamma(g, h)\Theta(g)\Theta(h)$ for some $\gamma(g, h) \in \mathbb{C}^\times$, i.e. the map $\Theta : g \mapsto \Theta(g)$ gives a projective representation of J, with factor set γ. We also have that $\Psi(gh) = \gamma(g, h)^{-1}\Psi(g)\Psi(h)$, and so $\Psi : g \mapsto \Psi(g)$ is a projective representation of J, with factor set γ^{-1}. Hence, for a fixed universal cover $\hat{J}$ of J, we can lift Θ and Ψ to linear representations of $\hat{J}$. Thus we can view A as a $\hat{J}$-module with character α, and B as a $\hat{J}$-module with character β. We can also inflate V to a $\hat{J}$-module, with character φ.

(ii) Recall that $J \cong \hat{J}/Z$ for some $Z \leq \mathbf{Z}(\hat{J})$. Let $\hat{P}$ be the full inverse image of P in $\hat{J}$, so that $\hat{P}/Z \cong P$, and let $Q := \mathbf{O}_p(\hat{P})$. Note that $Q \lhd \hat{J}$ and $\hat{P} = Q \times \mathbf{O}_{p'}(Z)$. In particular, $\hat{P}$ acts trivially on $\mathrm{Irr}(Q)$.

Recall the assumption that the J-module W is irreducible. Let λ_1 be an irreducible constituent of the P-character afforded by W, and let J_1 be the stabilizer of λ_1 in J. Since J_1/P is cyclic, λ_1 extends to J_1 and any irreducible character of J_1 lying above λ_1 restricts to λ_1 over P, see e.g. [Is, (11.22), (6.17)]. It follows by Clifford theory that the P-module W affords the character $\lambda_1 + \ldots + \lambda_s$, where $\{\lambda_1, \ldots, \lambda_s\}$ is a J/P-orbit on $\mathrm{Irr}(P)$. We will now inflate these characters to $\hat{P}$-characters, also denoted $\lambda_1, \ldots, \lambda_s$, with Z and $\mathbf{O}_{p'}(Z)$ in their kernels, and then have that

$$\varphi|_Q = c \cdot 1_Q + \sum_{i=1}^{s} \lambda_i, \text{ with } \{\lambda_1, \ldots, \lambda_s\} \text{ a } \hat{J}\text{-orbit on } \mathrm{Irr}(Q) \text{ and } c \in \mathbb{Z}_{\geq 1}. \tag{2.4.2}$$

Now write

$$\alpha|_Q = a \cdot 1_Q + \sum_{i=1}^{m} \alpha_i, \;\; \beta|_Q = b \cdot 1_Q + \sum_{j=1}^{n} \beta_j, \tag{2.4.3}$$

where $a, b, m, n \in \mathbb{Z}_{\geq 0}$, and $\alpha_i, \beta_j \in \mathrm{Irr}(Q) \smallsetminus \{1_Q\}$ not necessarily distinct. Since α is a $\hat{J}$-character and $Q \lhd \hat{J}$, $\{\alpha_1, \ldots, \alpha_m\}$ (if non-empty) is $\hat{J}$-stable, and similarly $\{\beta_1, \ldots, \beta_n\}$ is $\hat{J}$-stable if non-empty. In what follows we will refer to these two facts as $\hat{J}$-stability.

(iii) We will use the equality $\varphi|_Q = (\alpha|_Q)(\beta|_Q)$ to derive a contradiction. First we consider the case $a, m > 0$.

Suppose in addition that $b, n > 0$. Then $\varphi|_Q$ involves $b\sum_{i=1}^{m} \alpha_i + a\sum_{j=1}^{n} \beta_j$, and so, by $\hat{J}$-stability, it contains at least two Q-characters, each being a sum over some $\hat{J}$-orbit on $\mathrm{Irr}(Q) \smallsetminus \{1_Q\}$. This contradicts (2.4.2).

Now assume that $b > 0$ but $n = 0$. Then $\varphi|_Q = ab \cdot 1_P + b\sum_{i=1}^{m} \alpha_i$. Comparing the multiplicity of α_1 in $\varphi|_Q$ and using (2.4.2), we see that $b = 1$, and so $\dim(B) = \beta(1) = b = 1$, a contradiction.

Next we assume that $b = 0$, so that $n > 0$. Then

$$\varphi|_Q = a\sum_{j=1}^{n} \beta_j + \sum_{i,j} \alpha_i\beta_j.$$

Comparing the multiplicity of β_1 in $\varphi|_Q$ and using (2.4.2), we see that $a = 1$ and moreover all $\beta_1, \dots, \beta_n$ are pairwise distinct, whence $\{\beta_1, \dots, \beta_n\}$ is a $\hat{J}$-orbit by $\hat{J}$-stability. This in turn implies by (2.4.2) that $\{\beta_1, \dots, \beta_n\} = \{\lambda_1, \dots, \lambda_s\}$ and so

$$\alpha_i\beta_j = d_{ij}1_Q \text{ for some } d_{ij} \in \mathbb{Z}_{\geq 1} \text{ and for all } i, j. \tag{2.4.4}$$

Since $\alpha_i, \beta_j \in \mathrm{Irr}(Q)$, we observe that the multiplicity of 1_Q in $\alpha_i\beta_j$ is 0 if $\beta_j \neq \overline{\alpha}_i$ and 1 otherwise. Hence (2.4.4) can happen only when $\beta_j = \overline{\alpha}_i$ for all i, j and moreover $\alpha_i(1) = 1 = \beta_j(1)$. If $n \geq 2$, we would then have $\beta_1 = \overline{\alpha}_1 = \beta_2$, a contradiction. So $n = 1$ and $\dim(B) = n\beta_1(1) = 1$, again a contradiction.

(iv) In view of (iii), we have shown that $am = 0$ and so $bn = 0$ by symmetry.

Assume in addition that $m = 0$, so that $a > 0$. If $n = 0$, then (2.4.3) implies $\varphi|_Q = ab \cdot 1_Q$, contradicting (2.4.2). If $n > 0$, then $b = 0$, and $\varphi|_Q = a\sum_{j=1}^n \beta_j$, again contradicting (2.4.2).

Thus we must have $a = 0$, and so $b = 0$ by symmetry. Now, according to $\hat{J}$-stability, $\alpha|_Q$ is, say e times the sum over the $\hat{J}$-orbit $\{\alpha_1, \dots, \alpha_k\}$ of $\alpha_1 \in \mathrm{Irr}(Q)$. As mentioned above, $\hat{P} = Q \times \mathbf{O}_{p'}(Z)$ acts trivially on $\mathrm{Irr}(Q)$, so only the cyclic group $\langle x\rangle\hat{J}/\hat{P} \cong J/P$ acts on $\mathrm{Irr}(Q)$. Note that, in any transitive action of any finite abelian group, all the point stabilizers are the same. Thus, if $\hat{J}_1$ is the unique subgroup of $\hat{J}$ of index k that contains $\hat{P}$, then $\hat{J}_1$ is the stabilizer of α_1; moreover, we can write $\alpha_i = \alpha_1^{x^{i-1}}$ for $1 \leq i \leq k$, so that

$$\alpha|_Q = e\sum_{i=1}^k \alpha_1^{x^{i-1}}. \tag{2.4.5}$$

The same argument applies to β_Q. Furthermore, since 1_Q is contained in $(\alpha|_Q)(\beta|_Q)$, we may assume that $\beta_1 = \overline{\alpha}_1$. As α_1 and $\overline{\alpha}_1$ have the same stabilizer in $\hat{J}$, we see that the $\hat{J}$-orbit of β_1 is exactly

$$\{\overline{\alpha}_i = \overline{\alpha}_1^{x^{i-1}} \mid 1 \leq i \leq k\},$$

whence

$$\beta|_Q = f\sum_{i=1}^k \overline{\alpha}_1^{x^{i-1}}. \tag{2.4.6}$$

for some $f \in \mathbb{Z}_{\geq 1}$.

(v) Consider the case $k \geq 2$. Then $\varphi|_Q$ contains $ef\alpha_1\overline{\alpha}_1^x$ with $\alpha_1 \neq \alpha_1^x$. The latter implies that no irreducible constituent of $ef\alpha_1\overline{\alpha}_1^x$ can be 1_Q, and so $ef = 1$ by (2.4.2). Now, $\varphi|_Q$ contains the $\hat{J}$-stable character

$$\Sigma := \sum_{i=1}^{k-1} \alpha_1^{x^{i-1}}\overline{\alpha}_1^{x^i} + \alpha_1^{x^{k-1}}\overline{\alpha}_1,$$

and $[\varphi|_Q, 1_Q]_Q = k$ by (2.4.5) and (2.4.6). So (2.4.2) implies that $\sum_{i=1}^s \lambda_i$ is contained in Σ and $\varphi|_Q$ is contained in $k \cdot 1_Q + \Sigma$. Denoting $d := \alpha_1(1)$ and comparing degrees, we then get

$$k^2d^2 = \alpha(1)\beta(1) \leq k + \Sigma(1) = k + kd^2.$$

As $k \geq 2$, we conclude that $k = 2$, $d = 1$, $\dim(V) = \chi(1) = 4$. In this case, $k = 2$ divides the order of the p'-group J/P, so $p \neq 2$, and $\dim(T) = [\varphi|_Q, 1_Q]_Q = 2$. This contradicts our assumptions, cf. (a) and (c).

(vi) We have shown that $k = 1$, so that $\alpha|_Q = e\alpha_1$ and $\beta|_Q = f\overline{\alpha}_1$. Now if $\alpha_1(1) = 1$, then $\varphi|_Q = ef \cdot 1_Q$, contradicting (2.4.2). Hence $\alpha_1(1) > 1$. In this case, we have that $\alpha_1\overline{\alpha}_1$ is a character of degree > 1 that contains 1_Q with multiplicity 1, and so $\alpha_1\overline{\alpha}_1$ contains $1_Q + \mu$ for some $1_Q \neq \mu \in \mathrm{Irr}(Q)$. Comparing the multiplicity of μ using (2.4.2), we see that $ef = 1$. Thus $\chi(1) = \alpha_1(1)^2$, and so it is an even power of p, since α_1 is an irreducible character of the p-group P. Furthermore, from (2.4.2) we see that $1 = c \geq \dim(T)$, and so $\dim(T) = 1$. Now if $\dim(V) = 4$, then $\alpha_1(1) = 2$, whence $p = 2$, and this possibility is ruled by our assumptions, cf. (a) and (b). Hence we may assume that $\dim(V) \geq 9$, and so $d := \alpha_1(1) \geq 3$.

Recall that $Q \lhd \hat{J}$ and $\beta|_Q = \overline{\alpha}|_Q$ is irreducible. By Gallagher's theorem [Is, (6.17)], $\overline{\alpha} = \beta\lambda$ for some $\lambda \in \mathrm{Irr}(\hat{J}/Q)$ of degree 1. As T has dimension 1 and W is irreducible over $\hat{J}$, we see that $\alpha\overline{\alpha} = \chi\lambda$ is a sum of a linear character and an irreducible character of degree ≥ 8. It follows that $\alpha\overline{\alpha} - 1_G$ is irreducible. On the other hand, note that $\hat{J}$ is solvable. Moreover, if $2 \nmid d$, then $p > 2$ (as $\alpha|_Q$ is irreducible), and so Sylow

2-subgroups of J are cyclic, whence Sylow 2-subgroups of $\hat{J}$ are abelian. Applying Theorem 2.3, we arrive at a final contradiction. $\square$

Remark 2.5. As shown in [Ka-CC, 3.2 and 3.6] (or can be seen on the example of the dihedral group of order $2p$), there are modules V of dimension 4 and with tame part of dimension 2 which are tensor decomposable when $p > 2$. Furthermore, there are also tensor decomposable examples in dimension 4 with tame part of dimension 1 when $p = 2$. Indeed, consider the group $\mathrm{SL}_2(3) = Q \rtimes C$ with $Q = 2^{1+2}_-$ a quaternion group of order 8 and C cyclic of order 3 that acts transitively on $\mathrm{Irr}(P) \smallsetminus \{1_P\}$, where $P := Q/\mathbf{Z}(Q)$. Then $Q \rtimes C$ has a complex module W that affords a faithful irreducible character α of degree 2, and $(\alpha\overline{\alpha})|_Q$ is trivial on $\mathbf{Z}(Q) \cong C_2$ and equal to the regular character of P. This implies that $W \otimes W^*$ has tame part of dimension 1 and irreducible totally wild part of dimension 3. (Also note that $W \otimes W^*$ is indecomposable *as $P \rtimes C$-module*, even though $P \rtimes C$ preserves this tensor decomposition.)

3. The image of $I(\infty)$

In this section, we concentrate on the wild part

$$W = W(\psi, \chi_1, \ldots, \chi_n; \rho_1, \ldots, \rho_m)$$

of the $I(\infty)$-representation attached to a hypergeometric sheaf

$$\mathcal{H} = \mathcal{H}yp(\psi, \chi_1, \ldots, \chi_n; \rho_1, \ldots, \rho_m)$$

of type (n, m) with $n > m \geq 0$. We recall from [Ka-ESDE, 8.1.14] that for given ψ the isomorphism class of W as $I(\infty)$-representation depends only on the tame character $\prod_i \chi_i / \prod_j \rho_j$ and its rank $N := n - m$.

Lemma 3.1. *Suppose that $N := n - m$ is prime to p. If N is odd, suppose that $\prod_i \chi_i / \prod_j \rho_j = \mathbb{1}$. If N is even, suppose that $\prod_i \chi_i / \prod_j \rho_j = \chi_2$. Denote by f the multiplicative order of p in $(\mathbb{Z}/N\mathbb{Z})^\times$, so that $\mathbb{F}_{p^f}$ is the extension $\mathbb{F}_p(\mu_N)$ of $\mathbb{F}_p$ obtained by adjoining the N^{th} roots of unity. The image of the wild inertia group $P(\infty)$ is isomorphic to (the Pontryagin dual of the additive group of) $\mathbb{F}_{p^f}$, acting as the direct sum*

$$\oplus_{\zeta \in \mu_N(\mathbb{F}_{p^f})} \mathcal{L}_{\psi_N(\zeta x)}$$

of the N characters $x \mapsto \psi_{\mathbb{F}_{p^f}}(N\zeta x)$. The quotient group $I(\infty)/P(\infty)$ acts through its quotient $\mu_N(\mathbb{F}_{p^f})$ by permuting these characters: $\alpha \in \mu_N(\mathbb{F}_{p^f})$ maps $\mathcal{L}_{\psi_N(\zeta x)}$ to $\mathcal{L}_{\psi_N(\alpha\zeta x)}$. In particular, a primitive N^{th} root of unity cyclically permutes these N characters.

Proof. From [Ka-ESDE, 8.1.14], we see that our W occurs as the $I(\infty)$-representation attached to the Kloosterman sheaf

$$\mathcal{K}l(\psi; \text{all characters of order dividing } N),$$

which in turn is known [Ka-GKM, 5.6.2] to be geometrically isomorphic to the Kummer direct image $[N]_\star(\mathcal{L}_{\psi_N(x)})$. This direct image is $I(\infty)$-irreducible because the N multiplicative translates of $\mathcal{L}_{\psi_N(x)}$ by $\mu_N(\mathbb{F}_{p^f})$ are pairwise $I(\infty)$-inequivalent. The determination of the image of $P(\infty)$ is done exactly as in [Ka-RL-T-Co3, Lemma 1.2]. That the quotient group $I(\infty)/P(\infty)$ acts through its quotient $\mu_N(\mathbb{F}_{p^f})$ in the asserted way is implicit in the very definition of inducing a character from a normal subgroup of cyclic index N. $\square$

4. A particular class of hypergeometric sheaves

We remain in characterstic $p > 0$, with a chosen $\ell \neq p$, and a chosen nontrivial additive character ψ of $\mathbb{F}_p$. Fix two integers $A, B \geq 3$ with $\gcd(A, B) = 1$ and both A, B prime to p. We denote by

$$\mathcal{H}yp(\psi, A \times B; \mathbb{1})$$

the hypergeometric sheaf whose "upstairs" characters are the $(A-1)(B-1)$ characters of the form $\chi\rho$ with $\chi \neq \mathbb{1}, \chi^A = \mathbb{1}$ and $\rho \neq \mathbb{1}, \rho^B = \mathbb{1}$, and whose "downstairs" character is the single character $\mathbb{1}$. It is defined on $\mathbb{G}_m/\mathbb{F}_q$ for any finite extension of $\mathbb{F}_p$ containing the AB^{th} roots of unity. One knows [Ka-ESDE, 8.8.13] that $\mathcal{H}yp(\psi, A \times B; \mathbb{1})$ is pure of weight $(A-1)(B-1)$, and geometrically irreducible.

Lemma 4.1. *The determinant of $\mathcal{H}yp(\psi, A \times B; \mathbb{1})$ is geometrically trivial.*

Proof. Because both $A, B \geq 3$, the rank $(A-1)(B-1)$ is ≥ 4. Hence the wild part Wild of the $I(\infty)$-representation has dimension $(A-1)(B-1)-1 \geq 3 > 2$, so all slopes < 1, and hence det(Wild) must be tame. Therefore $\det(\mathcal{H}yp)$ is tame, and must be equal to the product of its $(A-1)(B-1)$ "upstairs" characters, the $\chi_i\rho_j$. At least one of A, B must be odd (because they are relatively prime), and therefore the product of the $\chi_i\rho_j$ is trivial. □

Lemma 4.2. *$\mathcal{H}yp(\psi, A\times B; \mathbb{1})$ is geometrically self dual precisely in the case $p = 2$, and in that case it is orthogonally self dual.*

Proof. This is immediate from [Ka-ESDE, 8.8.1 and 8.8.2], because, as noted above, at least one of A, B is odd, and hence $\mathcal{H}yp(\psi, A\times B; \mathbb{1})$ has even rank, but only one tame character "downstairs", namely $\mathbb{1}$. And it is obvious that the "upstairs" characters, the $\chi_i\rho_j$, are stable by complex conjugation (indeed by all of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$). □

In terms of Kubert's V function [Kub], we have the following criterion for finite monodromy.

Lemma 4.3. *Let $\mathbb{F}_q$ be a finite extension of $\mathbb{F}_p$ containing the AB^{th} roots of unity. Then the Tate twist*

$$\mathcal{H}yp(\psi, A\times B; \mathbb{1})((A-1)(B-1)/2)$$

has finite geometric and arithmetic monodromy groups if and only if, for all $x \in (\mathbb{Q}/\mathbb{Z})_{\text{prime to }p}$, we have

$$V(ABx) + V(x) + V(-x) \geq V(Ax) + V(Bx).$$

Equivalently, since this trivially holds for $x = 0$, the criterion is that for all nonzero $x \in (\mathbb{Q}/\mathbb{Z})_{\text{prime to }p}$, we have

$$V(ABx) + 1 \geq V(Ax) + V(Bx).$$

Proof. Entirely similar to the proof of [Ka-RL-T-Co2, Lemma 2.1], using the Hasse-Davenport relation to simplify the Mellin transform calculation [Ka-ESDE, 8.2.8] of the trace function of

$$\mathcal{H}yp(\psi, A\times B; \mathbb{1})((A-1)(B-1)/2).$$

□

Although it is possible to descend $\mathcal{H}yp(\psi, A\times B; \mathbb{1})$ to $\mathbb{G}_m/\mathbb{F}_p$, using [Ka-GKM, 8.8], we will instead give a "more computable" descent to $\mathbb{G}_m/\mathbb{F}_p(\zeta_A)$.

Lemma 4.4. *Denote by χ_i the $A-1$ nontrivial characters of order dividing A. The lisse sheaf $\mathcal{H}(\psi, A\times B)$ on $\mathbb{G}_m/\mathbb{F}_p(\zeta_A)$ whose trace function at a point $s \in K^\times$, $K/\mathbb{F}_p(\zeta_A)$ a finite extension, is given by*

$$s \mapsto \left(\frac{-1}{\#K}\right)^{A-1} \sum_{(t_i)_i\in\mathbb{G}_m(K)^{A-1}} \psi\Big(\frac{-\prod_i t_i}{s}\Big)\prod_i \chi_i(t_i) \sum_{(x_i)_i\in\mathbb{A}^1(K)^{A-1}} \psi_K\Big(B(\sum_i x_i) - \sum_i x_i^B/t_i\Big)$$

is a descent to $\mathbb{G}_m/\mathbb{F}_p(\zeta_A)$ of a constant field twist of $\mathcal{H}yp(\psi, A\times B; \mathbb{1})$.

Proof. Separate the numerator characters into packets $\chi_i \times$ (all allowed ρ), indexed by the $A-1$ nontrivial χ_i. Each of these packets is the list of characters for $\mathcal{L}_{\chi_i}\otimes\mathcal{K}l(\psi, \rho\neq\mathbb{1}, \rho^B = \mathbb{1})$. The multiplicative $\star_{,!}$ convolution of $\mathcal{L}_{\psi(-1/x)}$ with all of these is, by definition, the hypergeometric sheaf $\mathcal{H}yp(\psi, A\times B; \mathbb{1})$.

As proven in [Ka-RL-T-Co2, Lemma 1.2], the Kloosterman sheaf

$$\mathcal{K}l(\psi, \text{all nontrivial characters of order dividing } B)$$

has a descent to (a constant field twist of) the local system $\mathcal{B}_0$ on $\mathbb{G}_m/\mathbb{F}_p$ whose trace function is

$$t \in K^\times \mapsto -\sum_{x\in K} \psi_K(-x^B/t + Bx).$$

Convolving these $\mathcal{L}_{\chi_i}\otimes\mathcal{B}_0$ gives the assertion. □

Lemma 4.5. *The lisse sheaf $\mathcal{H}(\psi, A\times B)$ is pure of weight zero.*

Proof. The sheaf $\mathcal{H}yp(\psi, A \times B; \mathbb{1})$ is pure of weight $(A-1)(B-1)$. In replacing each

$$\mathcal{K}l(\psi, \text{all nontrivial characters of order dividing } B)$$

by $\mathcal{B}_0$, we save weight $(B-3)$ in each replacement, so all in all we save weight $(A-1)(B-3)$. The division by $(\#K)^{A-1}$ brings the weight down to zero. □

Lemma 4.6. *The trace function of $\mathcal{H}(\psi, A \times B)$ takes values in the field $\mathbb{Q}(\zeta_p)$.*

Proof. In the formula for the trace, we write the final summation

$$\sum_{(x_i)_i \in \mathbb{A}^1(K)^{A-1}} \psi_K\left(B(\sum_i x_i) - \sum_i x_i^B/t_i\right)$$

as

$$\prod_{1 \le i \le A-1} \left(\sum_{x \in K} \psi_K(Bx - x^B/t_i)\right),$$

a symmetric function of the t_i. The factor $\psi(-(\prod_i t_i)/s)$ is also a symmetric function of the t_i. So the formula for the trace at $s \in K^\times$ has the shape

$$\sum_{(t_i)_i \in \mathbb{G}_m(K)^{A-1}} (\prod_i \chi_i(t_i))(\text{Symmetric function of } (t_1, \ldots, t_{A-1})).$$

If we precompose with an automorphism of $\mathbb{G}_m^{A-1}$ given by a permutation of the variables, this sum (indeed any sum over $\mathbb{G}_m(K)^{A-1}$) does not change. But the effect of this on our sum is to correspondingly permute the χ_i. Thus in the formula for the trace, the sum does not change under any permutation of the χ_i. When we apply an element of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\zeta_p))$ to the sum, its only effect is to permute the χ_i (it permutes them among themselves because they are all the nontrivial characters of order dividing A, so as a set are Galois stable, even under $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$), or equivalently to permute the variables. Thus our sum is invariant under $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\zeta_p))$, so lies in $\mathbb{Q}(\zeta_p)$). □

Lemma 4.7. *If $p = 2$, then $\mathcal{H}(\psi, A \times B)$ has $\mathbb{Q}$-valued trace function, and we have inclusions*

$$G_{geom} \subset \mathrm{SO}_{(A-1)(B-1)}(\overline{\mathbb{Q}}_\ell), \quad G_{geom} \lhd G_{arith} \subset \mathrm{O}_{(A-1)(B-1)}(\overline{\mathbb{Q}}_\ell).$$

If we pass to the quadratic extension of $\mathbb{F}_p(\zeta_A)$, then we have

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

Proof. From Lemma 4.2, we know that $\mathcal{H}(\psi, A \times B)$ is, geometrically, orthogonally self dual. From Lemma 4.6 and Lemma 4.5, we know that $\mathcal{H}(\psi, A \times B)$ is pure of weight zero and has $\mathbb{Q}$-valued traces. This implies that $\mathcal{H}(\psi, A \times B)$ is arithmetically self dual. Because $\mathcal{H}(\psi, A \times B)$ is geometrically (and hence arithmetically) irreducible, the autoduality of $\mathcal{H}(\psi, A \times B)$ is unique up to a nonzero scalar factor. Being orthogonal geometrically, the autoduality of $\mathcal{H}(\psi, A \times B)$ must be orthogonal. Thus both G_{geom} and G_{arith} lie in $\mathrm{O}_{(A-1)(B-1)}(\overline{\mathbb{Q}}_\ell)$. By Lemma 4.7, we then get that G_{geom} lies in $\mathrm{SO}_{(A-1)(B-1)}(\overline{\mathbb{Q}}_\ell)$.

If G_{arith} lies in SO, we are done. If not, then the determinant of $\mathcal{H}(\psi, A \times B)$ is geometrically trivial, but takes values in ± 1, so must be the constant field twist $(-1)^{\deg}$, which disappears when we pass to the quadratic extension of $\mathbb{F}_p(\zeta_A)$. □

Lemma 4.8. *If $p \neq 2$, then $\mathcal{H}(\psi, A \times B)$ is not geometrically self dual, and we have inclusions*

$$G_{geom} \subset \mathrm{SL}_{(A-1)(B-1)}(\overline{\mathbb{Q}}_\ell), \quad G_{geom} \lhd G_{arith} \subset \mathrm{GL}_{(A-1)(B-1)}(\overline{\mathbb{Q}}_\ell).$$

If we pass to the degree $2p$ extension of $\mathbb{F}_p(\zeta_A)$, then we have

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

Proof. From Lemma 4.7, we know that $\mathcal{H}(\psi, A \times B)$ has geometrically trivial determinant, which gives the first assertion. From Lemma 4.6 and Lemma 4.5, we know that $\mathcal{H}(\psi, A \times B)$ is pure of weight zero and has $\mathbb{Q}(\zeta_p)$-valued traces. Therefore its determinant is of the form $\alpha^{\deg}$, for some $\alpha \in \mathbb{Q}(\zeta_p)$ which is a unit outside of the unique place over p, and all of whose complex absolute values are 1. Thus α is a root of unity in $\mathbb{Q}(\zeta_p)$, so of order dividing $2p$. So after passing to the degree $2p$ extension of $\mathbb{F}_p(\zeta_4)$, the determinant becomes arithmetically trivial as well. $\square$

5. A second class of hypergeometric sheaves

We remain in characterstic $p > 0$, with a chosen $\ell \neq p$, and a chosen nontrivial additive character ψ of $\mathbb{F}_p$. Fix an integer $A \geq 7$ which is prime to p. We denote by $\phi(A)$ the Euler ϕ function:

$$\phi(A) := \#(\mathbb{Z}/A\mathbb{Z})^\times = \text{ number of characters of order } A.$$

We denote by

$$\mathcal{H}yp(\psi, A^\times; \mathbb{1})$$

the hypergeometric sheaf whose "upstairs" characters are the $\phi(A)$ characters of order A, and whose "downstairs" character is the single character $\mathbb{1}$. It is defined on $\mathbb{G}_m/\mathbb{F}_q$ for any finite extension of $\mathbb{F}_p$ containing the A^{th} roots of unity. One knows [Ka-ESDE, 8.8.13] that $\mathcal{H}yp(\psi, A^\times; \mathbb{1})$ is pure of weight $\phi(A)$, and geometrically irreducible.

Lemma 5.1. *The determinant of $\mathcal{H}yp(\psi, A^\times; \mathbb{1})$ is geometrically trivial.*

Proof. Because $A \geq 7$, the rank $\phi(A)$ is ≥ 4. Hence the wild part Wild of the $I(\infty)$-representation has dimension $\geq 3 > 1$, so all slopes < 1, and hence $\det(\mathsf{Wild})$ must be tame. Therefore $\det(\mathcal{H}yp)$ is tame, and must be equal to the product of its $\phi(A)$ "upstairs" characters. Their product must be trivial, because they are stable by inversion and (because $A > 2$) none of them is χ_2. $\square$

We now explain the criterion for finite monodromy in terms of Kubert's V function. For simplicity, we will state it only in the case when A is divisible by precisely two distinct primes p_1 and p_2. Denote by $\Phi_N(X) \in \mathbb{Z}[X]$ the cyclotomic polynomial for the primitive N^{th} roots of unity. Then

$$\Phi_A(X) = \frac{(X^A - 1)(X^{A/(p_1p_2)} - 1)}{(X^{A/p_1} - 1)(X^{A/p_2} - 1)}.$$

Lemma 5.2. *Let $\mathbb{F}_q$ be a finite extension of $\mathbb{F}_p$ containing the A^{th} roots of unity. Suppose that A is divisible by precisely two distinct primes p_1 and p_2. Then the Tate twist*

$$\mathcal{H}yp(\psi, A^\times; \mathbb{1})(\phi(A)/2)$$

has finite geometric and arithmetic monodromy groups if and only if, for all $x \in (\mathbb{Q}/\mathbb{Z})_{\text{prime to } p}$, we have

$$V(Ax) + V(Ax/(p_1p_2)) + V(-x) \geq V(Ax/p_1) + V(Ax/p_2).$$

Proof. Entirely similar to the proof of [Ka-RL-T-Co2, Lemma 2.1], using the Hasse-Davenport relation to simplify the Mellin transform calculation [Ka-ESDE, 8.2.8] of the trace function of $\mathcal{H}yp(\psi, A^\times; \mathbb{1})(\phi(A)/2)$. $\square$

We now specialize further.

Lemma 5.3. *Suppose that the characteristic p is odd, and that $A = 4B$ with B an odd prime, $B \neq p$. The lisse sheaf $\mathcal{H}(\psi, (4B)^\times)$ on $\mathbb{G}_m/\mathbb{F}_p(\zeta_4)$ whose trace function at a point $s \in K^\times$, $K/\mathbb{F}_p(\zeta_4)$ a finite extension, is given by*

$$s \mapsto \left(\frac{-1}{\#K}\right)^2 \sum_{(u,v)\in\mathbb{G}_m(K)^2} \psi\left(\frac{-uv}{s}\right)\chi_4(u)\overline{\chi_4}(v) \sum_{(x,y)\in\mathbb{A}^1(K)^2} \psi_K\left(B(x+y) - \frac{x^B}{u} - \frac{y^B}{v}\right)$$

is a descent to $\mathbb{G}_m/\mathbb{F}_p(\zeta_4)$ of a constant field twist of $\mathcal{H}yp(\psi, A^\times; \mathbb{1})$.

Proof. Entirely similar to the proof of Lemma 4.4. $\square$

Lemma 5.4. *The lisse sheaf $\mathcal{H}(\psi, (4B)^\times)$ is pure of weight zero.*

Proof. Entirely similar to the proof of Lemma 4.5. $\square$

Lemma 5.5. *The trace function of $\mathcal{H}(\psi, (4B)^\times)$ takes values in the field $\mathbb{Q}(\zeta_p)$.*

Proof. Entirely similar to the proof of Lemma 4.6. ☐

Lemma 5.6. *For $\mathcal{H}(\psi,(4B)^\times)$ on $\mathbb{G}_m/\mathbb{F}_p(\zeta_4)$, we have*

$$G_{geom} \subset \mathrm{SL}_{2(B-1)}(\overline{\mathbb{Q}}_\ell).$$

After passing to the degree $2p$ extension of $\mathbb{F}_p(\zeta_4)$, we have

$$G_{geom} \lhd G_{arith} \subset \mathrm{SL}_{2(B-1)}(\overline{\mathbb{Q}}_\ell).$$

Proof. The first assertion is just Lemma 5.1, that $\det(\mathcal{H}(\psi,(4B)^\times))$ is geometrically constant. In view of Lemmas 5.5 and 5.4, $\det(\mathcal{H}(\psi,(4B)^\times))$ is of the form $\alpha^{\deg}$ for some $\alpha\in\mathbb{Q}(\zeta_p)$ which is a unit outside of the unique place over p, and all of whose complex absolute values are 1. Thus α is a root of unity in $\mathbb{Q}(\zeta_p)$, so of order dividing $2p$. So after passing to the degree $2p$ extension of $\mathbb{F}_p(\zeta_4)$, the determinant becomes arithmetically trivial as well. ☐

6. Theorems of finite monodromy

In this section, we will use Lemmas 4.3 and 5.2 to prove finite monodromy. We will freely use results of [Ka-RL, §4], showing how the condition on Kubert's V function can be interpreted in terms of the following function $[-]_{p,r}$, which is defined for any fixed prime p. For any integer $x\ge 0$, we define

$$[x]_{p,\infty} := \text{the sum of the digits of the } p\text{-adic expansion of } x,$$

using the usual digits $\{0,1,2,\dots,p-1\}$. For every integer $r\ge 1$ we define $[x]_{p,r}:=[x]_{p,\infty}$ if $1\le x\le p^r-1$, and we extend the definition to every integer x by imposing that $[x]_{p,r}=[y]_{p,r}$ if $(p^r-1)\mid(x-y)$.

6.1. The case $p=2$.

In this section we fix $p=2$ and let $[x]_r:=[x]_{2,r}$.

Theorem 6.1. *In characteristic $p=2$, the lisse sheaf $\mathcal{H}(\psi,3\times 13)$ on $\mathbb{G}_m/\mathbb{F}_4$ has finite G_{arith} and finite G_{geom}.*

Proof. By Lemma 4.3, we must show that

$$V(39x)+1\ge V(3x)+V(13x),$$

for all nonzero $x\in(\mathbb{Q}/\mathbb{Z})_{\text{prime to }2}$. If $x\in\frac{1}{39}\mathbb{Z}$ we check it by hand. If $39x\ne 0$, then by the change of variable $x\mapsto -x$ and the relation $V(x)+V(-x)=1$ for $x\ne 0$, it is equivalent to

$$V(39x)\le V(3x)+V(13x)$$

which, applying the formula $V(3x)+1=V(x)+V(x+\frac{1}{3})+V(x+\frac{2}{3})$, is equivalent to

$$V\left(13x+\frac{1}{3}\right)+V\left(13x+\frac{2}{3}\right)\le V(x)+V\left(x+\frac{1}{3}\right)+V\left(x+\frac{2}{3}\right).$$

In terms of the $[-]_r$ function, we need to show that, for all **even** $r\ge 2$ and all integers $0<x<2^r-1$ we have

$$\left[13x+\frac{2^r-1}{3}\right]_r+\left[13x+\frac{2(2^r-1)}{3}\right]_r\le [x]_r+\left[x+\frac{2^r-1}{3}\right]_r+\left[x+\frac{2(2^r-1)}{3}\right]_r. \tag{6.1.1}$$

For even $r\ge 2$, let $A_r=\frac{2^r-1}{3}$ and $B_r=\frac{2(2^r-1)}{3}$. For odd $r\ge 1$, let $A_r=\frac{2^{r+1}-1}{3}$ and $B_r=\frac{2^r-2}{3}$. Note that, for $1\le s<r$, we have

$$\begin{array}{lll} A_r=2^sA_{r-s}+A_s, & B_r=2^sB_{r-s}+B_s & \text{if } s \text{ is even}\\ A_r=2^sB_{r-s}+A_s, & B_r=2^sA_{r-s}+B_s & \text{if } s \text{ is odd}\end{array}$$

For a non-negative integer x, let $[x]$ denote the sum of the 2-adic digits of x.

Lemma 6.2. *Let $r \geq 1$ and let $0 \leq x < 2^r$ an integer. Then*

$$[13x + A_r] + [13x + B_r] \leq [x] + [x + A_r] + [x + B_r] + 4.$$

Moreover, if $r \geq 4$ and the first four digits of x are not 0100, 1000 or 1001, then

$$[13x + A_r] + [13x + B_r] \leq [x] + [x + A_r] + [x + B_r] + 2.$$

If $x < 2^{r-2}$ (i.e. the first two of the r 2-adic digits of x are 0) then

$$[13x + A_r] + [13x + B_r] \leq [x] + [x + A_r] + [x + B_r] + 1.$$

Finally, if the first four digits of x are 1010, then

$$[13x + A_r] + [13x + B_r] \leq [x] + [x + A_r] + [x + B_r].$$

Proof. We proceed by induction on r: for $r \leq 14$ one checks it by computer. Let $r \geq 15$ and $0 \leq x < 2^r$, and consider the 2-adic expansion of x. By adding leading 0's as needed, we will assume that it has exactly r digits.

In all cases below we will follow one of these two procedures: in the first one, for some $1 \leq s \leq r - 4$, we write $x = 2^s y + z$ with $y < 2^{r-s}$, $z < 2^s$. Assume s is even (otherwise, just interchange A_{r-s} and B_{r-s} below). Let C be the total number of digit carries in the sums $13x + A_r = 2^s(13y + A_{r-s}) + (13z + A_s)$ and $13x + B_r = 2^s(13y + B_{r-s}) + (13z + B_s)$ and D the total number of digit carries in the sums $x + A_r = 2^s(y + A_{r-s}) + (z + A_s)$ and $x + B_r = 2^s(y + B_{r-s}) + (z + B_s)$, and let $\lambda_s(z) := [13z + A_s] + [13z + B_s] - [z] - [z + A_s] - [z + B_s]$. If $C - D - \lambda_s(z) \geq 0$, then

$$\begin{aligned}
(6.2.1)\qquad [13x + A_r] + [13x + B_r] &= [2^s(13y + A_{r-s}) + (13z + A_s)] + [2^s(13y + B_{r-s}) + (13z + B_s)] \\
&= [13y + A_{r-s}] + [13z + A_s] + [13y + B_{r-s}] + [13z + B_s] - C \leq \\
&\leq [y] + [y + A_{r-s}] + [y + B_{r-s}] + 4 + [z] + [z + A_s] + [z + B_s] + \lambda_s(z) - C \leq \\
&\leq [y] + [y + A_{r-s}] + [y + B_{r-s}] + 4 + [z] + [z + A_s] + [z + B_s] - D = \\
&= [2^s y + z] + [2^s(y + A_{r-s}) + (z + A_s)] + [2^s(y + B_{r-s}) + (z + B_s)] + 4 = [x] + [x + A_r] + [x + B_r] + 4
\end{aligned}$$

by induction. Moreover, the first four digits of x and y are the same, so the better inequalities hold for x whenever they do for y.

In the second procedure, for some $1 \leq s \leq r - 4$, we write $x = 2^s y + z$ with $y < 2^{r-s}$, $z < 2^s$. Again we assume s is even (otherwise, just interchange A_{r-s} and B_{r-s} below). For some $0 < s' < s$ (which we also assume even without loss of generality) we find some $z' < 2^{s'}$ such that the following conditions hold: if $z + A_s$ (respectively $z + B_s$, $13z + A_s$, $13z + B_s$) has $s + \alpha$ digits (resp. $s + \beta$, $s + \gamma$, $s + \delta$), then $z' + A_{s'}$ (resp. $z' + B_{s'}$, $13z' + A_{s'}$, $13z' + B_{s'}$) has $s' + \alpha$ digits (resp. $s' + \beta$, $s' + \gamma$, $s' + \delta$) and the first α digits of $z + A_s$ and $z' + A_{s'}$ (resp. the fist β digits of $z + B_s$ and $z' + B_{s'}$, the first γ digits of $13z + A_s$ and $13z' + A_{s'}$, the first δ digits of $13z + B_s$ and $13z' + B_{s'}$) coincide. Moreover, we require that $\lambda_s(z) \leq \lambda_{s'}(z')$.

Let $r' = r - s + s'$ and $x' = 2^{s'} y + z' < 2^{r'}$. Then the total number C of digit carries in the sums $13x + A_r = 2^s(13y + A_{r-s}) + (13z + A_s)$ and $13x + B_r = 2^s(13y + B_{r-s}) + (13z + B_s)$ is the same as the total number of digit carries in the sums $13x' + A_{r'} = 2^{s'}(13y + A_{r-s}) + (13z' + A_{s'})$ and $13x' + B_{r'} = 2^{s'}(13y + B_{r-s}) + (13z' + B_{s'})$, and the total number D of digit carries in the sums $x + A_r = 2^s(y + A_{r-s}) + (z + A_s)$ and $x + B_r = 2^s(y + B_{r-s}) + (z + B_s)$ is the same as the total number of digit carries in the sums $x' + A_{r'} = 2^{s'}(y + A_{r-s}) + (z' + A_{s'})$ and $x' + B_{r'} = 2^{s'}(y + B_{r-s}) + (z' + B_{s'})$, so we have

$$\begin{aligned}
(6.2.2)\qquad [13x + A_r] + [13x + B_r] &= [2^s(13y + A_{r-s}) + (13z + A_s)] + [2^s(13y + B_{r-s}) + (13z + B_s)] \\
&= [13y + A_{r-s}] + [13z + A_s] + [13y + B_{r-s}] + [13z + B_s] - C \leq \\
&\leq [13y + A_{r-s}] + [13z' + A_{s'}] + [13y + B_{r-s}] + [13z' + B_{s'}] - C + \\
&\quad + [z] + [z + A_s] + [z + B_s] - [z'] - [z' + A_{s'}] - [z' + B_{s'}] = \\
&= [13x' + A_{r'}] + [13x' + B_{r'}] + [z] + [z + A_s] + [z + B_s] - [z'] - [z' + A_{s'}] - [z' + B_{s'}] \leq \\
&\leq [x'] + [x' + A_{r'}] + [x' + B_{r'}] + 4 + [z] + [z + A_s] + [z + B_s] - [z'] - [z' + A_{s'}] - [z' + B_{s'}] = \\
&= [y] + [y + A_{r-s}] + [y + B_{r-s}] + 4 + [z] + [z + A_s] + [z + B_s] - D = \\
&= [x] + [x + A_r] + [x + B_r] + 4
\end{aligned}$$

by induction. Moreover, the first four digits of x and x' are the same, so the better inequalities hold for x whenever they do for x'.

Case 1: $x \equiv 0 \mod 2$. We apply (6.2.1) with $s = 1$, so $z = 0$ and $C = D = \lambda_s(z) = 0$.

Case 2: The last three digits of x are 001.

Case 2a: The last 4 digits of x are 0001. Take $s = 4$ in (6.2.1), so $z = 1 = 0001_2$. Then D is clearly 0 and $\lambda_s(z) = 0$, so $C - D - \lambda_s(z) = C \geq 0$.

Case 2b: The last 5 digits of x are 01001. Take $s = 3$, so $z = 1 = 001_2$ and $y \equiv 1 \mod 4$. Here $A_3 + 1 = 6$ and $B_3 + 1 = 3$ are both < 8, so $D = 0$. On the other hand, $13 + A_3 = 18 = 10010_2$ and the last two digits of $13y + B_{r-3}$ are 11, so $C \geq 1$. Therefore $C - D - \lambda_s(z) \geq 1 - 1 = 0$.

Case 2c: The last six digits of x are 011001. We can apply (6.2.2) with $s = 6$, $z = 25 = 011001_2$, $s' = 5$ and $z' = 13 = 01101_2$, so $\lambda_s(z) = \lambda_{s'}(z') = 2$.

Case 2d: The last seven digits of x are 0111001. We can apply (6.2.2) with $s = 7$, $z = 57 = 0111001_2$, $s' = 6$ and $z' = 31 = 011111_2$, so $\lambda_s(z) = \lambda_{s'}(z') = 0$.

Case 2e: The last nine digits of x are 001111001. We apply (6.2.2) with $s = 9$, $z = 121 = 001111001_2$, $s' = 2$ and $z' = 1 = 01_2$, so $\lambda_s(z) = 1 < \lambda_{s'}(z') = 3$.

Case 2f: The last ten digits of x are 0101111001. We apply (6.2.1) with $s = 5$, so $z = 25 = 11001_2$, $\lambda_s(z) = 1$ and $D = 1$. Since $13 \cdot 25 + A_5 = 101011010_2$ and the last five digits of $13y + B_{r-5}$ are 11001, we get at least two digit carries in the sum $13x + A_r = 2^5(13y + B_{r-5}) + (13z + A_5)$, so $C - D - \lambda_s(z) \geq 2 - 1 - 1 = 0$.

Case 2g: The last ten digits of x are 1101111001. We can apply (6.2.2) with $s = 10$, $z = 889 = 1101111001_2$, $s' = 7$ and $z' = 109 = 1101101_2$, so $\lambda_s(z) = \lambda_{s'}(z') = 2$.

Case 2h: The last nine digits of x are 011111001. We can apply (6.2.2) with $s = 9$, $z = 249 = 011111001_2$, $s' = 8$ and $z' = 121 = 01111001_2$, so $\lambda_s(z) = \lambda_{s'}(z') = 1$.

Case 2i: The last nine digits of x are 111111001. We apply (6.2.1) with $s = 5$, so $z = 25 = 11001_2$, $\lambda_s(z) = 1$ and $D = 1$. Since $13 \cdot 25 + A_5 = 101011010_2$, $13 \cdot 25 + B_5 = 101001111_2$ and the last four digits of $13y + B_{r-5}$ and $13y + A_{r-5}$ are 1101 and 1000 respectively, we get at least one digit carry in each of the sums $13x + A_r = 2^5(13y + B_{r-5}) + (13z + A_5)$ and $13x + B_r = 2^5(13y + A_{r-5}) + (13z + B_5)$, so $C - D - \lambda_s(z) \geq 2 - 1 - 1 = 0$.

Case 3: The last $r - 4$ digits of x contain two consecutive 0's. Suppose that the right-most ones are located in positions $t - 1, t$ for $t \geq 2$ (counting from the right). If $t = 2$, x is even and we apply case 1. If $t = 3$ we apply case 2. Suppose that $t \geq 4$.

Case 3a: Either previous two digits are not 11 or the next two digits are 11. Take $s = t$ in (6.2.1). Then $\lambda_s(z) \leq 1$, since $z < 2^{s-2}$. Assume without loss of generality that s is even. Both $z + A_s$ and $z + B_s$ are $< 2^s$, so $D = 0$. If $t = 4$ and the two digits after the 0's are 10 we can apply case 1. Otherwise, since we picked the right-most consecutive 0's, the following digits are at least 101 (that is, $z \geq 2^{s-3} + 2^{s-5}$). It follows that $13z + A_s$ and $13z + B_s$ both have $s + 2$ digits, the first two being 10 or 11. Then, if the second-to-last digit of either $13y + A_{r-s}$ or $13y + B_{r-s}$ is 1 (which is the case if the last two digits of y are not 11) or the last two digits of y are 11 and the first two digits of $13z + B_s$ are 11 (which is the case if the third and fourth digits of z are 11), we get at least one digit carry in one of the sums $13x + A_r = 2^s(13y + A_{r-s}) + (13z + A_s)$ or $13x + B_r = 2^s(13y + B_{r-s}) + (13z + B_s)$, so $C \geq 1$ and $C - D - \lambda_s(z) \geq 0$.

Case 3b: The last five digits of x are 00101. We apply (6.2.1) with $s = 5$ and $z = 5 = 00101_2$, so $D = 0$ and $\lambda_s(z) = -1$.

Case 3c: The last six digits of x are 001011. We apply (6.2.1) with $s = 6$ and $z = 5 = 001011_2$, so $D = 0$ and $\lambda_s(z) = 0$.

Case 3d: The previous two digits are 11, and the next four digits are 1010. Take $s = t - 2$ in (6.2.1), so the last four digits of y are 1100 and $\lambda_s(z) \leq 0$ by induction. If z has no two consecutive 1's (that is, $z = 101010\ldots$), there are no digit carries in the sums $x + A_r = 2^s(y + A_{r-s}) + (z + A_s)$ and $x + B_r = 2^s(y + B_{r-s}) + (z + B_s)$, so $D = 0$ and we are done. Otherwise $D = 1$. Note that $13 \cdot \overbrace{10\ldots10}^{t\times 10} 11 + \overbrace{01\ldots01}^{(t+1)\times 01} = 1001\overbrace{00\ldots0}^{2t-1}100$ so (if s is even) $13z + A_s$ has $s + 4$ digits, the first four being 1001. Then there is one digit carry in the sum $13x + A_r = 2^s(13y + A_{r-s}) + (13z + A_s)$, so $C - D - \lambda_s(z) \geq 1 - 1 - 0 = 0$.

Case 3e: In all remaining cases, the previous two digits are 11 and the next four are 1011 (since we picked the right-most consecutive 0's). Take $s = t - 4$ in (6.2.1), then the last six digits of y are 110010 and the first two digits of z are 11. There is no digit carry in the sum $x + B_r = 2^s(y + B_{r-s}) + (z + B_s)$ and at most three digit carries in the sum $x + A_r = 2^s(y + A_{r-s}) + (z + A_s)$, so $D \leq 3$.

Suppose first that $s < 6$. Then $\lambda_s(z) \leq 1$ and $\lambda_s(z) = 1$ only for $s = 4$, $z = 13 = 1101_2$ and $s = 5$, $z = 25 = 11001_2$, $z = 26 = 11010_2$ or $z = 27 = 11011_2$, as one can check directly. On the other hand, $13z + A_s$ and $13z + B_s$ have s digits, the first four being 1010, 1011, 1100 or 1101, and the last six digits of $13y + A_{r-s}$ and $13y + B_{r-s}$ are 011111 and 110100 respectively. Then we get at least three digit carries in the sum $13x + A_r = 2^s(13y + A_{r-s}) + (13z + A_s)$. Moreover, in all cases where $\lambda_s(z) = 1$ the first four digits of $13z + A_s$ are 1010 or 1011, so we get at least four digit carries in the sum above. In any case, $C - D - \lambda_s(z) \geq 3 - 3 = 0$.

If $s \geq 6$, then the first six digits of z are at least 110101, and the first four digits of $13z + A_s$ and $13z + B_s$ are 1011, 1100 or 1101. If the first four digits of $13z + A_s$ are 1011 we get five digit carries in the sum in the sum $13x + A_r = 2^s(13y + A_{r-s}) + (13z + A_s)$. If the first four digits of $13z + A_s$ are 1100 or 1101, then so are the first four digits of $13z + B_s$, and we get at least three digit carries in the sum $13x + A_r = 2^s(13y + A_{r-s}) + (13z + A_s)$ and at least two more in the sum $13x + B_r = 2^s(13y + B_{r-s}) + (13z + B_s)$. In either case, we have $C - D - \lambda_s(z) \geq 5 - 3 - 2 = 0$.

This concludes the proof of case 3.

Case 4: The last two digits of x are 11. Suppose that the last string of consecutive 1's has length $m \geq 2$.

Case 4a: $m \geq 5$, that is, the last five digits of x are 11111. We apply (6.2.1) with $s = 3$, so $z = 7$. Then there is one digit carry in the sum $x + A_r = 8(y + B_{r-3}) + (7 + A_3)$ and no digit carries in the sum $x + B_r = 8(y + A_{r-3}) + (7 + B_3)$. If there is a 0 before the five 1's, then we can assume that the last four digits of y are 1011 (otherwise we would have two consecutive 0's and we could apply case 2). Then $13 \cdot 7 + A_3 = 1100000_2$ and the last four digits of $13y + B_{r-3}$ are 1001, so there is one digit carry in the sum $13x + A_r = 8(13y + B_{r-3}) + (13 \cdot 7 + A_3)$. If there is a 1 before the five 1's, then the last three digits of $13y + B_{r-3}$ are 101, so again there is (at least) one digit carry in the above sum. Therefore $C - D - \lambda_s(z) \geq 1 - 1 - 0 = 0$.

Case 4b: $m = 4$, that is, the last five digits of x are 01111. We can assume that the previous digit is a 1 (otherwise we apply case 2). We apply (6.2.1) with $s = 2$, so $z = 3$ and y ends with 1011. Then there is one digit carry in the sum $x + B_r = 4(y + B_{r-2}) + (3 + B_2)$ and no digit carries in the sum $x + A_r = 4(y + A_{r-2}) + (3 + A_2)$. Also, $13 \cdot 3 + B_2 = 41 = 101001_2$, and the last four digits of $13y + B_{r-2}$ are 1001, so there is one digit carry in the sum $13x + B_r = 4(13y + B_{r-2}) + (13 \cdot 3 + B_2)$. Therefore $C - D - \lambda_s(z) = 1 - 1 - 0 = 0$.

Case 4c: $m = 3$, that is, the last four digits of x are 0111. Again, we can assume that the previous digit is a 1. We apply (6.2.1) with $s = 1$, so $z = 1$ and y ends with 1011. Then there is one digit carry in the sum $x + A_r = 2(y + B_{r-1}) + (1 + A_1)$ and no digit carries in the sum $x + B_r = 2(y + A_{r-1}) + (1 + B_1)$. Also, $13 \cdot 1 + A_1 = 14 = 1110_2$, and the last four digits of $13y + B_{r-1}$ are 1001, so there are at least four digit carries in the sum $13x + A_r = 2(13y + B_{r-1}) + (13 \cdot 1 + A_1)$. Therefore $C - D - \lambda_s(z) \geq 4 - 1 - 3 = 0$.

The remaining subcases of case 4 have $m = 2$, that is, the last four digits of x are 1011.

Case 4d: The last six digits of x are 111011. We apply (6.2.1) with $s = 4$, so $z = 11 = 1011_2$ and y ends with 11. Then there is one digit carry in the sum $x + B_r = 16(y + B_{r-4}) + (11 + B_4)$ and no digit carries in the sum $x + A_r = 16(y + A_{r-4}) + (11 + B_4)$. Also, $13 \cdot 11 + B_4 = 10011001_2$, and the last two digits of $13y + B_{r-4}$ are 01, so there is at least one digit carry in the sum $13x + B_r = 16(13y + B_{r-4}) + (13 \cdot 11 + B_4)$. Therefore $C - D - \lambda_s(z) \geq 1 - 1 - 0 = 0$.

Case 4e: The last six digits of x are 011011. We apply (6.2.1) with $s = 3$, so $z = 3 = 011_2$ and y ends with 011. Then there is one digit carry in the sum $x + A_r = 8(y + B_{r-3}) + (3 + A_3)$ and no digit carries in the sum $x + B_r = 8(y + A_{r-3}) + (3 + B_3)$. Also, $13 \cdot 3 + A_3 = 44 = 101100_2$, $13 \cdot 3 + B_3 = 41 = 101001_2$, and the last three digits of $13y + A_{r-3}$ and $13y + B_{r-3}$ are 100 and 001 respectively, so there is at least one digit carry in each of the sums $13x + A_r = 8(13y + B_{r-3}) + (13 \cdot 3 + A_3)$ and $13x + B_r = 8(13y + A_{r-3}) + (13 \cdot 3 + B_3)$. Therefore $C - D - \lambda_s(z) \geq 2 - 1 - 1 = 0$.

Case 4f: The last six digits of x are 101011. We can apply (6.2.2) with $s = 6$, $z = 43 = 101011_2$, $s' = 4$ and $z' = 11 = 1011_2$, since $\lambda_s(z) = -1 < 0 = \lambda_{s'}(z')$.

This ends the proof for case 4. It remains to check the case where x ends with 01. By case 2, we can assume that the previous digit is a 1.

Case 5: The last four digits of x are 0101. We apply (6.2.1) with $s = 3$, so $z = 5 = 101_2$ and y is even. Then there are no digit carries in either sum $x+A_r = 8(y+B_{r-3})+(5+A_3)$ or $x+B_r = 8(y+A_{r-3})+(5+B_3)$, so $C - D - \lambda_s(z) = C + 1 > 0$.

Case 6: The last five digits of x are 11101. We apply (6.2.1) with $s = 1$, so $z = 1$ and y ends with 1110. Then there are no digit carries in the sums $x+A_r = 2(y+B_{r-1})+(1+A_1)$ and $x+B_r = 2(y+A_{r-1})+(1+B_1)$. Also, $13\cdot 1+B_1 = 13 = 1101_2$, and the last four digits of $13y+A_{r-1}$ are 1011, so there are at least three digit carries in the sum $13x+B_r = 2(13y+A_{r-1})+(13\cdot 1+B_1)$. Therefore $C-D-\lambda_s(z) \geq 3-0-3 = 0$.

In the remaining cases, the last six digits of x are 101101.

Case 7: The last nine digits of x are 111101101. We apply (6.2.1) with $s = 4$, so $z = 13 = 1101_2$ and y ends with 11110. Then there are two digit carries in the sum $x + A_r = 16(y + A_{r-4}) + (13 + A_4)$ and no digit carries in the sum $x + B_r = 16(y + B_{r-4}) + (13 + B_4)$. Also, $13 \cdot 13 + A_4 = 10101110_2$, and the last five digits of $13y + A_{r-4}$ are 11011, so there are at least three digit carries in the sum $13x + A_r = 16(13y + A_{r-4}) + (13 \cdot 13 + A_4)$. Therefore $C - D - \lambda_s(z) \geq 3 - 2 - 1 = 0$.

Case 8: The last nine digits of x are 011101101. By case 2, we can assume that the previous digit is a 1. We apply (6.2.1) with $s = 6$, so $z = 45 = 101101_2$ and y ends with 1011. Then there is one digit carry in the sum $x + B_r = 64(y + B_{r-6}) + (45 + B_6)$ and no digit carries in the sum $x + A_r = 64(y+A_{r-6})+(45+A_6)$. Also, $13\cdot 45+B_6 = 1001110011_2$ and the least four digits of $13y+B_{r-6}$ are 1001, so there are at least two digit carries in the sum $13x + B_r = 64(13y + B_{r-6}) + (13 \cdot 45 + B_6)$. Therefore $C - D - \lambda_s(z) \geq 2 - 1 - 1 = 0$.

Case 9: The last eight digits of x are 01101101. By case 2, we can assume that the previous digit is a 1. We apply (6.2.2) with $s = 9$, $z = 365 = 101101101_2$, $s' = 6$ and $z' = 45 = 101101_2$. Here $\lambda_s(z) = \lambda_{s'}(z') = 1$.

Case 10: The last seven digits of x are 0101101.By case 2, we can assume that the previous digit is a 1. We apply (6.2.2) with $s = 8$, $z = 173 = 10101101_2$, $s' = 4$ and $z' = 11 = 1011_2$. Here $\lambda_s(z) = \lambda_{s'}(z') = 0$.

□

Corollary 6.3. *Let $r \geq 2$ be even and let $0 < x < 2^r - 1$ an integer. Then*

$$[13x + A_r]_r + [13x + B_r]_r \leq [x]_r + [x + A_r]_r + [x + B_r]_r + 5.$$

Proof. If $x = A_r = \frac{2^r-1}{3}$ or $x = B_r = \frac{2(2^r-1)}{3}$ it is obviuos. Otherwise, the 2-adic expansion of x contains two consecutive 0's or two consecutive 1's.

In the first case, multiplying by a suitable power of 2 we can assume that the first two digits of x are 00, that is, $x < 2^{r-2}$. Then $x + A_r$ and $x + B_r$ are both $< 2^r$, so

$$[13x + A_r]_r + [13x + B_r]_r \leq [13x + A_r] + [13x + B_r] \leq$$

$$\leq [x] + [x + A_r] + [x + B_r] + 4 = [x]_r + [x + A_r]_r + [x + B_r]_r + 4.$$

In the second case, multiplying by a suitable power of 2 we can assume that the last two digits of x are 11. Then $x + A_r$ ends with 10 and has at most $r + 1$ digits. If $x + A_r < 2^r$ then $[x + A_r]_r = [x + A_r]$, and if $x + A_r \geq 2^r$ then $[x + A_r]_r = [x + A_r - 2^r + 1]_r = [x + A_r - 2^r + 1] = [x + A_r] - 1 + 1 = [x + A_r]$. On the other hand, $x + B_r$ ends with 01 and has at most $r + 1$ digits. If $x + B_r < 2^r$ then $[x + B_r]_r = [x + B_r]$, and if $x + B_r \geq 2^r$ then $[x + B_r]_r = [x + B_r - 2^r + 1]_r = [x + B_r - 2^r + 1] = [x + B_r] - 1$, since there is one digit carry in the sum $(x + B_r) + 1$. In any case,

$$[13x + A_r]_r + [13x + B_r]_r \leq [13x + A_r] + [13x + B_r] \leq$$

$$\leq [x] + [x + A_r] + [x + B_r] + 4 \leq [x]_r + [x + A_r]_r + [x + B_r]_r + 5.$$

□

We can now finish the proof of Theorem 6.1. By the numerical Hasse-Davenport relation [Ka-RL-T-Co3, Lemma 2.10], using that $A_{kr} = \frac{2^{kr}-1}{2^r-1}A_r$ and $B_{kr} = \frac{2^{kr}-1}{2^r-1}B_r$ we get, applying the previous corollary to $x' := \frac{2^{kr}-1}{2^r-1}x$,

$$[13x' + A_{kr}]_{kr} + [13x' + B_{kr}]_{kr} \leq [x']_{kr} + [x' + A_{kr}]_{kr} + [x' + B_{kr}]_{kr} + 5 \Rightarrow$$
$$\Rightarrow [13x + A_r]_r + [13x + B_r]_r \leq [x]_r + [x + A_r]_r + [x + B_r]_r + \frac{5}{k}$$

and we conclude by taking $k \to \infty$. □

6.2. **The case $p = 3$.** In this section we fix $p = 3$ and let $[x]_r := [x]_{3,r}$.

Theorem 6.4. *In characteristic $p = 3$, the lisse sheaf $\mathcal{H}(\psi, 4 \times 5)$ on $\mathbb{G}_m/\mathbb{F}_9$ has finite G_{arith} and finite G_{geom}.*

Proof. By Lemma 4.3, we must show that

$$V(20x) + 1 \geq V(4x) + V(5x),$$

for all nonzero $x \in (\mathbb{Q}/\mathbb{Z})_{\text{prime to } p}$. If $x \in \frac{1}{20}\mathbb{Z}$ we check it by hand, otherwise, just as in the proof of Theorem 6.1, it is equivalent to

$$V(20x) \leq V(4x) + V(5x)$$

which, applying the duplication formula, is equivalent to

$$V\left(5x + \frac{1}{2}\right) + V\left(10x + \frac{1}{2}\right) \leq V(x) + V\left(x + \frac{1}{2}\right) + V\left(2x + \frac{1}{2}\right).$$

In terms of the $[-]_r$ function, we need to show that, for all $r \geq 2$ and all integers $0 < x < 3^r - 1$ we have

$$\left[5x + \frac{3^r-1}{2}\right]_r + \left[10x + \frac{3^r-1}{2}\right]_r \leq [x]_r + \left[x + \frac{3^r-1}{2}\right]_r + \left[2x + \frac{3^r-1}{2}\right]_r. \tag{6.4.1}$$

For a non-negative integer x, let $[x]$ denote the sum of the 3-adic digits of x.

Lemma 6.5. *Let $r \geq 1$ and let $0 \leq x < 3^r$ an integer. Then*

$$\left[5x + \frac{3^r-1}{2}\right] + \left[10x + \frac{3^r-1}{2}\right] \leq [x] + \left[x + \frac{3^r-1}{2}\right] + \left[2x + \frac{3^r-1}{2}\right] + 2.$$

Moreover, if the first two digits of x are not 10, 11 or 21, then we have the better inequality

$$\left[5x + \frac{3^r-1}{2}\right] + \left[10x + \frac{3^r-1}{2}\right] \leq [x] + \left[x + \frac{3^r-1}{2}\right] + \left[2x + \frac{3^r-1}{2}\right].$$

Proof. We proceed by induction on r: for $r \leq 7$ one checks it by computer. Let $r \geq 8$ and $0 \leq x < 3^r$, and consider the 3-adic expansion of x. By adding leading 0's as needed, we will assume that it has exactly r digits. Let $A_r = \frac{3^r-1}{2}$.

In all cases below we will follow one of these two procedures: in the first one, for some $s \leq r - 2$, we write $x = 3^s y + z$ with $y < 3^{r-s}$, $3 < 2^s$. Let C be the total number of digit carries in the sums $5x + A_r = 3^s(5y + A_{r-s}) + (5z + A_s)$ and $10x + A_r = 3^s(10y + A_{r-s}) + (10z + A_s)$ and D the total number of digit carries in the sums $x + A_r = 3^s(y + A_{r-s}) + (z + A_s)$ and $2x + A_r = 3^s(2y + A_{r-s}) + (2z + A_s)$, and let $\lambda_s(z) = [5z + A_s] + [10z + A_s] - [z] - [z + A_s] - [2z + A_s]$. If $2(C - D) - \lambda_s(z) \geq 0$, then

$$\begin{aligned}
[5x + A_r] + [10x + A_r] &= [3^s(5y + A_{r-s}) + (5z + A_s)] + [3^s(10y + A_{r-s}) + (10z + A_s)] = \\
&= [5y + A_{r-s}] + [5z + A_s] + [10y + A_{r-s}] + [10z + A_s] - 2C \leq \\
&\leq [y] + [y + A_{r-s}] + [2y + A_{r-s}] + 2 + [z] + [z + A_s] + [2z + A_s] + \lambda_s(z) - 2C \leq \\
&\leq [y] + [y + A_{r-s}] + [2y + A_{r-s}] + 2 + [z] + [z + A_s] + [2z + A_s] - 2D = \\
&= [3^s y + z] + [3^s(y + A_{r-s}) + (z + A_s)] + [3^s(2y + A_{r-s}) + (2z + A_s)] + 2 = [x] + [x + A_r] + [2x + A_r] + 2
\end{aligned} \tag{6.5.1}$$

by induction. Moreover, the first two digits of x and y are the same, so the better inequality holds for x whenever they do for y.

In the second procedure, for some $1 \le s \le r-2$, we write $x = 3^s y + z$ with $y < 3^{r-s}$, $z < 3^s$. For some $0 < s' < s$ we find some $z' < 3^{s'}$ such that the following conditions hold: if $z + A_s$ (respectively $2z + A_s$, $5z + A_s$, $10z + A_s$) has $s + \alpha$ digits (resp. $s + \beta$, $s + \gamma$, $s + \delta$), then $z' + A_{s'}$ (resp. $2z' + A_{s'}$, $5z' + A_{s'}$, $10z' + A_{s'}$) has $s' + \alpha$ digits (resp. $s' + \beta$, $s' + \gamma$, $s' + \delta$) and the first α digits of $z + A_s$ and $z' + A_{s'}$ (resp. the fist β digits of $2z + A_s$ and $2z' + A_{s'}$, the first γ digits of $5z + A_s$ and $5z' + A_{s'}$, the first δ digits of $10z + A_s$ and $10z' + A_{s'}$) coincide. Moreover, we require that $\lambda_s(z) \le \lambda_{s'}(z')$.

Let $r' = r - s + s'$ and $x' = 3^{s'} y + z' < 3^{r'}$. Then the total number C of digit carries in the sums $5x + A_r = 3^s(5y + A_{r-s}) + (5z + A_s)$ and $10x + A_r = 3^s(10y + A_{r-s}) + (10z + A_s)$ is the same as the total number of digit carries in the sums $5x' + A_{r'} = 3^{s'}(5y + A_{r-s}) + (5z' + A_{s'})$ and $10x' + A_{r'} = 3^{s'}(10y + A_{r-s}) + (10z' + A_{s'})$, and the total number D of digit carries in the sums $x + A_r = 3^s(y + A_{r-s}) + (z + A_s)$ and $2x + A_r = 3^s(2y + A_{r-s}) + (2z + A_s)$ is the same as the total number of digit carries in the sums $x' + A_{r'} = 3^{s'}(y + A_{r-s}) + (z' + A_{s'})$ and $2x' + A_{r'} = 3^{s'}(2y + A_{r-s}) + (2z' + A_{s'})$, so we have

$$
\begin{aligned}
(6.5.2) \qquad [5x + A_r] + [10x + A_r] &= [3^s(5y + A_{r-s}) + (5z + A_s)] + [3^s(10y + A_{r-s}) + (10z + B_s)] \\
&= [5y + A_{r-s}] + [5z + A_s] + [10y + A_{r-s}] + [10z + A_s] - 2C \le \\
&\le [5y + A_{r-s}] + [5z' + A_{s'}] + [10y + A_{r-s}] + [10z' + A_{s'}] - 2C + \\
&\quad + [z] + [z + A_s] + [2z + A_s] - [z'] - [z' + A_{s'}] - [2z' + A_{s'}] = \\
&= [5x' + A_{r'}] + [10x' + A_{r'}] + [z] + [z + A_s] + [2z + A_s] - [z'] - [z' + A_{s'}] - [2z' + A_{s'}] \le \\
&\le [x'] + [x' + A_{r'}] + [2x' + A_{r'}] + 2 + [z] + [z + A_s] + [2z + A_s] - [z'] - [z' + A_{s'}] - [2z' + A_{s'}] = \\
&= [y] + [y + A_{r-s}] + [2y + A_{r-s}] + 2 + [z] + [z + A_s] + [2z + A_s] - D = \\
&= [x] + [x + A_r] + [2x + A_r] + 2
\end{aligned}
$$

by induction. Moreover, the first two digits of x and x' are the same, so the better inequality holds for x whenever they do for x'.

Case 1: $x \equiv 0 \mod 3$. We apply (6.5.1) with $s = 1$, so $z = 0$ and $C = D = \lambda_s(z) = 0$.

Case 2: The last two digits of x are 01 or 02. We apply (6.5.1) with $s = 2$, so $z \le 2$ and $D = \lambda_s(z) = 0$ (since $2z + A_2 \le 8 < 3^2$). Therefore $2(C - D) - \lambda_s(z) = 2C \ge 0$.

Case 3: The last three digits of x are 011. We apply (6.5.1) with $s = 3$, so $z = 4 = 011_3$ and $D = \lambda_s(z) = 0$ (since $2z + A_3 = 21 < 3^3$). Therefore $2(C - D) - \lambda_s(z) = 2C \ge 0$.

Case 4: The last three digits of x are 111. We apply (6.5.1) with $s = 1$, so $z = 1 = 1_3$, $\lambda_s(z) = 1$ and $D = 0$ (since $2y + A_{r-1}$ ends with a 0). On the other hand, $10y + A_{r-1}$ ends with 22 and $10z + A_1 = 102_3$, so $C \ge 1$. Therefore $2(C - D) - \lambda_s(z) \ge 2 - 1 = 1$.

Case 5: The last $r - 1$ digits of x contain the strings 00 or 01. Pick s such that the first two digits of z are 00 or 01. Then $D = 0$ and $\lambda_s(z) \le 0$, so $2(C - D) - \lambda_s(z) \ge 2C \ge 0$. If $s = r - 1$ and the first digit of x is not 1 then we have the better inequality (since $\lambda_1(0) = \lambda_1(2) = 0$).

Case 6: The last $r - 1$ digits of x contain the string 10. Pick s such that the last digit of y is 1 and the first digit of z is 0. Then the last digit of $2y + A_{r-s}$ is 0, so $D = 0$ and $\lambda_s(z) \le 0$. Therefore $2(C - D) - \lambda_s(z) \ge 2C \ge 0$.

Case 7: x contains one of the strings 1202 or 2202. Pick s such that the last two digits of y are 12 or 22 and the first two digits of z are 02. Then the last two digits of $2y + A_{r-s}$ are 02 or 12, so there is at most one digit carry in the sum $2x + A_r = 3^s(2y + A_{r-s}) + (2z + A_s)$, and $D \le 1$. On the other hand, the last digit of $5y + A_{r-s}$ is 2, and $3^s < 5z + A_s < 3^{s+1}$, so there is at least one digit carry in the sum $5x + A_r = 3^s(5y + A_{r-s}) + (5z + A_s)$. Therefore $2(C - D) - \lambda \ge 2(1 - 1) - 0 = 0$.

Case 8: The last four digits of x are 0211. Using cases 5,6 and 7, we can assume that the previous three digits are 202. We apply (6.5.2) with $s = 7$, $z = 1642 = 2020211_3$, $s' = 5$ and $z' = 184 = 20211_3$. Here $\lambda_s(z) = -2 < 0 = \lambda_{s'}(z')$.

Case 9: The last four digits of x are 1211. Let t be the number of consecutive 1's before the 2. We apply (6.5.1) with $s = 3$, so $z = 22 = 211_3$ and $\lambda_s(z) = 2$. There are t digit carries in the sum $x + A_r = 27(y + A_{r-3}) + (z + A_3)$ and no digit carry in $2x + A_r = 27(2y + A_{r-3}) + (2z + A_3)$, so $D = t$. On the other hand, the last t digits of $5y + A_{r-3}$ and $10y + A_{r-3}$ are $\overbrace{22\ldots22}^{t-1}0$ and $\overbrace{11\ldots11}^{t-3}022$ respectively, and $5 \cdot 22 + A_3 = 123 = 11120_3$ and $10 \cdot 22 + A_3 = 233 = 22122_3$, so we get $t-1$ digit carries in the sum $5x + A_r = 27(5y + A_{r-3}) + (5z + A_3)$ and at least two more in the sum $10x + A_r = 27(10y + A_{r-3}) + (10z + A_3)$. Therefore $2(C - D) - \lambda_s(z) \geq 2(t + 1 - t) - 2 = 0$.

Case 10: The last four digits of x are 2211. We apply (6.5.1) with $s = 2$, so $z = 4 = 11_3$, $\lambda_s(z) = 2$ and the last two digits of $2y + A_{r-2}$ are 02, so $D = 1$. On the other hand, $5y + A_{r-2}$ ends with 22 and $5z + A_2 = 24 = 220_3$, so $C \geq 2$. Therefore $2(C - D) - \lambda_s(z) \geq 2 - 2 = 0$.

Case 11: The last three digits of x are 021 or 022. Using cases 5,6 and 7, we can assume that the previous three digits are 202. We apply (6.5.2) with $s = 6$, $z = 547 = 202021_3$ or $z = 548 = 202022_3$, $s' = 4$, and $z' = 61 = 2021_3$ or $z' = 62 = 2022_3$ respectively. Here $\lambda_s(z) = -3 < -1 = \lambda_{s'}(z')$ in the $z = 547$ case and $\lambda_s(z) = -2 < 0 = \lambda_{s'}(z')$ in the $z = 548$ case.

Case 12: The last three digits of x are 121. This is similar to case 9, with $s = 2$, $z = 7 = 21_3$ and $\lambda_s(z) = 1$ now. Here $5 \cdot 7 + A_2 = 39 = 1110_3$ and $10 \cdot 7 + A_2 = 74 = 2202_3$, so we get $t - 1$ digit carries in the sum $5x + A_r = 9(5y + A_{r-2}) + (5z + A_2)$ and at least two more in the sum $10x + A_r = 9(10y + A_{r-2}) + (10z + A_2)$. Therefore $2(C - D) - \lambda_s(z) \geq 2(t + 1 - t) - 1 = 1$.

Case 13: The last three digits of x are 221. We apply (6.5.1) with $s = 1$, so $z = 1 = 1_3$ and $\lambda_s(z) = 1$. There is only one digit carry in the sum $2x + A_r = 3(2y + A_{r-1}) + (2z + A_1)$, so $D = 1$. The last two digits of $5y + A_{r-2}$ are 22, so we get at least two digit carries in the sum $5x + A_r = 3(5y + A_{r-1}) + (5z + A_1)$. Therefore $2(C - D) - \lambda_s(z) \geq 2(2 - 1) - 1 = 1$.

Case 14: The last two digits of x are 12. Let t be the number of consecutive 1's before the last digit. We apply (6.5.1) with $s = 1$, so $z = 2 = 2_3$ and $\lambda_s(z) = 0$. There are t digit carries in the sum $x + A_r = 3(y + A_{r-1}) + (z + A_1)$ and no digit carry in $2x + A_r = 3(2y + A_{r-1}) + (2z + A_1)$, so $D = t$. On the other hand, the last t digits of $5y + A_{r-1}$ and $10y + A_{r-1}$ are $\overbrace{22\ldots22}^{t-1}0$ and $\overbrace{11\ldots11}^{t-3}022$ respectively, and $5 \cdot 2 + A_1 = 11 = 102_3$ and $10 \cdot 2 + A_1 = 21 = 210_3$, so we get $t - 1$ digit carries in the sum $5x + A_r = 3(5y + A_{r-1}) + (5z + A_1)$ and at least one more in the sum $10x + A_r = 3(10y + A_{r-1}) + (10z + A_1)$. Therefore $2(C - D) - \lambda_s(z) \geq 2(t - t) - 0 = 0$.

Case 15: The last three digits of x are 122. Let t be the number of consecutive 1's before the 22. We apply (6.5.1) with $s = 2$, so $z = 8 = 22_3$ and $\lambda_s(z) = -2$. There are t digit carries in the sum $x + A_r = 9(y+A_{r-2})+(z+A_2)$ and no digit carry in $2x+A_r = 9(2y+A_{r-2})+(2z+A_2)$, so $D = t$. On the other hand, the last t digits of $5y + A_{r-2}$ are $\overbrace{22\ldots22}^{t-1}0$, and $5 \cdot 8 + A_2 = 44 = 1122_3$, so we get $t - 1$ digit carries in the sum $5x+A_r = 9(5y+A_{r-2})+(5z+A_2)$. Therefore $2(C-D)-\lambda_s(t) \geq 2(t-1-t)+2 = 0$.

Case 16: The last three digits of x are 222. We apply (6.5.1) with $s = 1$, so $z = 2 = 2_3$ and $\lambda_s(z) = 0$. There is only one digit carry in the sum $2x + A_r = 3(2y + A_{r-1}) + (2z + A_1)$, so $D = 1$. The last two digits of $5y + A_{r-2}$ are 22, so we get at least one digit carry in the sum $5x + A_r = 3(5y + A_{r-1}) + (5z + A_1)$. Therefore $2(C - D) - \lambda_s(z) \geq 2(1 - 1) = 0$.

□

Corollary 6.6. *Let $r \geq 1$ and let $0 < x < 2^r - 1$ an integer. Then*

$$[5x + A_r]_r + [10x + A_r]_r \leq [x]_r + [x + A_r]_r + [2x + A_r]_r + 6.$$

Proof. If $x = A_r = \frac{3^r-1}{2}$ or r is even and $x = \frac{3^r-1}{4}$ or $x = \frac{3(3^r-1)}{4}$ then $[x]_r + [x + A_r]_r + [2x + A_r]_r = 4r$ and the inequality is obvious. Otherwise, the 3-adic expansion of x contains two consecutive digits with are not 11, 02 or 20. Multiplying x by a suitable power of 3, we can assume that they are the last two digits.

Note that $x + A_r$ has at most $r + 1$ digits, and if it has $r + 1$ then the first one is 1. In that case, $[x + A_r]_r = [x + A_r - 3^r + 1] = [x + A_r + 1] - 1$. Since the last two digits of x are not 11, the last two digits of $x + A_r$ are not 22, so there is at most one digit carry in the sum $(x + A_r) + 1$. Therefore $[x + A_r + 1] - 1 \geq [x + A_r] - 2$. In any case, we get $[x + A_r]_r \geq [x + A_r] - 2$.

$2x + A_r$ has at most $r + 1$ digits. If it has $r + 1$, let $a \in \{1, 2\}$ be the first one. Then $[2x + A_r]_r = [2x + A_r - a \cdot 3^r + a] = [2x + A_r + a] - a$. Since the last two digits of x are not 02 or 20, the last two digits of $2x + A_r$ are not 21 or 22, so there is at most one digit carry in the sum $(2x + A_r) + a$. Therefore $[2x + A_r + a] - a \geq [2x + A_r] - 2$. In any case, we get $[2x + A_r]_r \geq [2x + A_r] - 2$.

So we have

$$[5x + A_r]_r + [10x + A_r]_r \leq [5x + A_r] + [10x + A_r] \leq$$
$$\leq [x] + [x + A_r] + [2x + A_r] + 2 \leq [x]_r + [x + A_r]_r + 2 + [2x + A_r]_r + 2 + 2$$

□

We conclude the proof of (6.4.1) by using the numerical Hasse-Davenport formula as in Theorem 6.1. □

Theorem 6.7. *In characteristic $p = 3$, the lisse sheaf $\mathcal{H}(\psi, 28^\times)$ on $\mathbb{G}_m/\mathbb{F}_9$ has finite G_{arith} and finite G_{geom}.*

Proof. By Lemma 5.2, we must show that

$$V(28x) + V(2x) + V(-x) \geq V(4x) + V(14x),$$

for all $x \in (\mathbb{Q}/\mathbb{Z})_{\text{prime to } 3}$. If $x \in \frac{1}{28}\mathbb{Z}$ we check it by hand, otherwise, just as in the proof of Theorem 6.1, it is equivalent to

$$V(28x) + V(2x) \leq V(x) + V(4x) + V(14x)$$

which, applying the duplication formula, is equivalent to

$$V\left(14x + \frac{1}{2}\right) \leq V(x) + V\left(2x + \frac{1}{2}\right).$$

In terms of the $[-]_r$ function, we need to show that, for all $r \geq 2$ and all integers $0 < x < 3^r - 1$ we have

$$\left[14x + \frac{3^r - 1}{2}\right]_r \leq [x]_r + \left[2x + \frac{3^r - 1}{2}\right]_r. \tag{6.7.1}$$

For a non-negative integer x, let $[x]$ denote the sum of the 3-adic digits of x.

Lemma 6.8. *Let $r \geq 1$ and let $0 \leq x < 3^r$ an integer. Then*

$$\left[14x + \frac{3^r - 1}{2}\right] \leq [x] + \left[2x + \frac{3^r - 1}{2}\right] + 1.$$

Proof. We proceed by induction on r: for $r \leq 3$ one checks it by computer. Let $r \geq 4$ and $0 \leq x < 3^r$, and consider the 3-adic expansion of x. By adding leading 0's as needed, we will assume that it has exactly r digits. Let $A_r = \frac{3^r - 1}{2}$.

In all cases below we will follow this procedure: for some $s \leq r - 2$, we write $x = 3^s y + z$ with $y < 3^{r-s}$, $z < 3^s$. Let C be the total number of digit carries in the sum $14x + A_r = 3^s(14y + A_{r-s}) + (14z + A_s)$ and D the total number of digit carries in the sum $2x + A_r = 3^s(2y + A_{r-s}) + (2z + A_s)$, and let $\lambda_s(z) = [14z + A_s] - [z] - [2z + A_s]$. If $2(C - D) - \lambda_s(z) \geq 0$, then

$$[14x + A_r] = [3^s(14y + A_{r-s}) + (14z + A_s)] = [14y + A_{r-s}] + [14z + A_s] - 2C \leq \tag{6.8.1}$$
$$\leq [y] + [2y + A_{r-s}] + 1 + [z] + [2z + A_s] + \lambda_s(z) - 2C \leq [y] + [2y + A_{r-s}] + 1 + [z] + [2z + A_s] - 2D =$$
$$= [3^s y + z] + [3^s(2y + A_{r-s}) + (2z + A_s)] + 1 = [x] + [2x + A_r] + 1$$

by induction.

Case 1: $x \equiv 0 \mod 3$. We apply (6.8.1) with $s = 1$, so $z = 0$ and $C = D = \lambda_s(z) = 0$.

Case 2: The last two digits of x are 01. We apply (6.8.1) with $s = 1$, so $z = 1$, $\lambda_s(z) = 1$ and $D = 0$. Here $14z + A_1 = 15 = 120_3$, and the last digit of $14y + A_{r-1}$ is 1, so $C \geq 1$. Therefore $2(C - D) - \lambda_s(z) \geq 2 - 0 - 1 = 1$.

Case 3: The last three digits of x are 011 or 111. We apply (6.8.1) with $s = 2$, so $z = 4 = 11_3$ and $\lambda_s(z) = 0$. Here $2z + A_2 = 12 = 110_3$ and the last digit of $2y + A_{r-2}$ is 1 or 0, so $D = 0$. Therefore $2(C - D) - \lambda_s(z) = 2C \geq 0$.

Case 4: The last four digits of x are 0211. We apply (6.8.1) with $s = 3$, so $z = 22 = 211_3$ and $\lambda_s(z) = 0$. Suppose that the last t digits of y are $2020\ldots20$ (if t is even) or $020\ldots20$ (if t is odd) and the previous one is not 0 (if t is even) or 2 (if t is odd). Then $2z + A_3 = 57 = 2010_3$ and the last t digits of $2y + A_{r-3}$ are $\overbrace{22\ldots22}^{t-1}1$ with the previous one (if it exists) different than 2, so $D = t$. On the other hand, $14z + A_3 = 321 = 102220_3$ and the last t digits of $14y + A_{r-3}$ are $\overbrace{22\ldots22}^{t-3}121$, so $C \geq t$ and therefore $2(C - D) - \lambda_s(t) \geq 2(t - t) = 0$.

Case 5: The last four digits of x are 1211. We apply (6.8.1) with $s = 3$, so $z = 22 = 211_3$ and $\lambda_s(z) = 0$. Here $2z + A_3 = 57 = 2010_3$ and the last digit of $2y + A_{r-3}$ is 0, so $D = 0$. Therefore $2(C - D) - \lambda_s(z) = 2C \geq 0$.

Case 6: The last four digits of x are 2211. We apply (6.8.1) with $s = 2$, so $z = 4 = 11_3$ and $\lambda_s(z) = 0$. Here $2z + A_2 = 12 = 110_3$ and the last two digits of $2y + A_{r-2}$ are 02, so $D = 1$. On the other hand, $14z + A_2 = 60 = 2020_3$ and the last two digits of $14y + A_{r-2}$ are 22, so $C \geq 1$. Therefore $2(C - D) - \lambda_s(z) \geq 2(1 - 1) = 0$.

Case 7: The last three digits of x are 021. Here we can proceed as in case 4 if we take $s = 2$ and $z = 7 = 21_3$ (so $\lambda_s(z) = -1$), since $2z + A_2 = 18 = 200_3$ and $14z + A_2 = 102 = 10210_3$.

Case 8: The last three digits of x are 121. We apply (6.8.1) with $s = 2$, so $z = 7 = 21_3$ and $\lambda_s(z) = -1$. Since the last digit of $2y + A_{r-2}$ is 0, we have $D = 0$, so $2(C - D) - \lambda_s(z) = 2C + 1 > 0$.

Case 9: The last three digits of x are 221. We apply (6.8.1) with $s = 1$, so $z = 1 = 1_3$ and $\lambda_s(z) = 1$. The last two digits of $2y + A_{r-1}$ are 02, so $D = 1$. On the other hand, the last two digits of $14y + A_{r-1}$ are 22 and $14z + A_1 = 15 = 120_3$, so $C \geq 2$. Therefore $2(C - D) - \lambda_s(z) \geq 2(2 - 1) - 1 > 0$.

Case 10: The last two digits of x are 02 or 12, or the last three digits are 122 or 222. We apply (6.8.1) with $s = 1$, so $z = 2 = 2_3$ and $\lambda_s(z) = -2$. Here $2z + A_1 = 5 = 12_3$ and the last two digits of $2y + A_{r-1}$ are not 22, so $D \leq 1$. Therefore $2(C - D) - \lambda_s(z) \geq 2(C - 1) + 2 = 2C \geq 0$.

Case 11: The last three digits of x are 022. We apply (6.8.1) with $s = 2$, so $z = 8 = 22_3$ and $\lambda_s(z) = -2$. Suppose as in case 4 that the last t digits of y are $2020\ldots20$ (if t is even) or $020\ldots20$ (if t is odd) and the previous one is not 0 (if t is even) or 2 (if t is odd). Then $2z + A_2 = 20 = 202_3$, so $D = t$. On the other hand, $14z + A_2 = 116 = 11022_3$, so $C \geq t-1$ and therefore $2(C-D)-\lambda_s(z) \geq 2(t-1-t)+2 = 0$.

□

Corollary 6.9. *Let $r \geq 1$ and let $0 < x < 3^r - 1$ an integer. Then*

$$[14x + A_r]_r \leq [x]_r + [2x + A_r]_r + 3.$$

Proof. If r is even and $x = \frac{3^r-1}{4}$ or $x = \frac{3(3^r-1)}{4}$ then $[2x+A_r]_r = 2r$ and the inequality is obvious. Otherwise, the 3-adic expansion of x contains two consecutive digits with are not 02 or 20. Multiplying x by a suitable power of 3, we can assume that they are the last two digits.

Note that $2x + A_r$ has at most $r + 1$ digits. If it has $r + 1$, let $a \in \{1, 2\}$ be the first one. Then $[2x + A_r]_r = [2x + A_r - a \cdot 3^r + a] = [2x + A_r + a] - a$. Since the last two digits of x are not 02 or 20, the last two digits of $2x + A_r$ are not 21 or 22, so there is at most one digit carry in the sum $(2x + A_r) + a$. Therefore $[2x + A_r + a] - a \geq [2x + A_r] - 2$. In any case, we get $[2x + A_r]_r \geq [2x + A_r] - 2$.

So we have

$$[14x + A_r]_r \leq [14x + A_r] \leq$$

$$\leq [x] + [2x + A_r] + 1 \leq [x]_r + [2x + A_r]_r + 3.$$

□

We conclude the proof of (6.7.1) by using the numerical Hasse-Davenport formula as in Theorem 6.1. □

7. Determination of some finite complex linear groups

Theorem 7.1. *Let $V = \mathbb{C}^{12}$ and let $G < \mathcal{G} := \mathrm{GL}(V)$ be a finite irreducible subgroup. Suppose that all the following conditions hold:*

(i) *V is primitive and tensor indecomposable;*
(ii) *G contains a subgroup N of the form $N = C_3^5 \rtimes C_{11}$, with C_{11} acting nontrivially on $Q := \mathbf{O}_3(N) = C_3^5$.*

Then $G = \mathbf{Z}(G)H$ with $H \cong 6.\mathsf{Suz}$ in one of its two (up to equivalence) complex conjugate irreducible representations of degree 12.

Proof. (a) By the assumption, the G-module V is irreducible, primitive and tensor indecomposable. Since $\dim(V) = 12$, it cannot be tensor induced. Hence, we can apply [GT2, Proposition 2.8] to obtain a finite subgroup $H < \mathrm{SL}(V)$ with $\mathbf{Z}(\mathcal{G})G = \mathbf{Z}(\mathcal{G})H$ which is almost quasisimple, that is, $S \lhd H/\mathbf{Z}(H) \leq \mathrm{Aut}(S)$ for some finite non-abelian simple group S. By [GT2, Lemma 2.5], the layer $L = E(H)$ (which in this case is just the last term of the derived series of the complete inverse image of S in H) is a finite quasisimple group acting irreducibly on V, whence $\mathbf{Z}(L) \leq \mathbf{Z}(H)$ by Schur's Lemma.

Condition (ii) implies that the subgroup C_{11} of N acts irreducibly on Q (considered as an $\mathbb{F}_3$-module), and so it acts fixed-point-freely on $Q \smallsetminus \{1\}$. In particular, $Q \cap \mathbf{Z}(\mathcal{G}) = 1$. By the construction of H in the proof of [GT2, Proposition 2.8], it contains the subgroup

$$Q_1 := \{\alpha g \in \mathrm{SL}(V) \mid g \in Q, \alpha \in \mathbb{C}^\times\}$$

such that $\mathbf{Z}(\mathcal{G})Q = \mathbf{Z}(\mathcal{G})Q_1$. It follows that

$$Q_1/(Q_1 \cap \mathbf{Z}(H)) = Q_1/(Q_1 \cap \mathbf{Z}(\mathcal{G})) \cong Q/(Q \cap \mathbf{Z}(\mathcal{G})) \cong Q \cong C_3^5,$$

which implies that the almost simple group $H/\mathbf{Z}(H) \leq \mathrm{Aut}(S)$ has 3-rank at least 5.

(b) Applying the main result of [H-M] to L, we now arrive at one of the following possibilities.

- $S = \mathsf{A}_{13}$, A_6, $\mathrm{SL}_3(3)$, $\mathrm{PSL}_2(11)$, $\mathrm{PSL}_2(13)$, $\mathrm{PSL}_2(23)$, $\mathrm{PSL}_2(25)$, $\mathrm{SU}_3(4)$, $\mathrm{PSp}_4(5)$, $G_2(4)$, or M_{12}. In all of these cases, the 3-rank of $\mathrm{Aut}(S)$ is less than 5, see [ATLAS], a contradiction.
- $L = 6.\mathsf{Suz}$. In this case, since outer automorphisms of L do not fix the isomorphism class of any complex irreducible representation of degree 12 of L (in fact, it fuses the two central elements of order 3 of L which act nontrivially on V), we see that $H/\mathbf{C}_H(L) \cong L/\mathbf{Z}(L)$, and so $H = \mathbf{Z}(H)L$ and $L = [L, L] = [H, H]$. As $\mathbf{Z}(\mathcal{G})G = \mathbf{Z}(\mathcal{G})H$, we conclude that $G = \mathbf{Z}(G)L$, as stated. ☐

Theorem 7.2. *Let $V = \mathbb{C}^{24}$ and let $G < \mathrm{O}(V)$ be a finite irreducible subgroup. Suppose that all the following conditions hold:*

(i) *V is primitive and tensor indecomposable;*
(ii) *G contains a subgroup N of the form $N = C_2^{11} \rtimes C_{23}$, with C_{23} acting nontrivially on $Q := \mathbf{O}_2(N) \cong C_2^{11}$.*

Then $G \cong 2.\mathsf{Co}_1$ in its unique (up to equivalence) irreducible representation of degree 24.

Proof. (a) By the assumption, the G-module V is irreducible, primitive and tensor indecomposable. Since $\dim(V) = 24$, it cannot be tensor induced. Hence, G is almost quasisimple by [GT2, Proposition 2.8], and so $S \lhd G/\mathbf{Z}(G) \leq \mathrm{Aut}(S)$ for some finite non-abelian simple group S. By [GT2, Lemma 2.5], the layer $L = E(G)$ (which in this case again is the last term of the derived series of the complete inverse image of S in G) is a finite quasisimple group acting irreducibly on V, whence $\mathbf{Z}(L) \leq \mathbf{Z}(G) \leq C_2$ by Schur's Lemma.

Condition (ii) implies that the subgroup C_{23} of N acts irreducibly on Q (considered as an $\mathbb{F}_2$-module), and so it acts fixed-point-freely on $Q \smallsetminus \{1\}$. In particular, $Q \cap \mathbf{Z}(G) = 1$. It follows that

$$Q/(Q \cap \mathbf{Z}(G)) \cong Q \cong C_2^{11},$$

which implies that the almost simple group $G/\mathbf{Z}(G) \leq \mathrm{Aut}(S)$ has 2-rank at least 11.

(b) Applying the main result of [H-M] to L, we now arrive at one of the following possibilities.

- $S = \mathsf{A}_7$, A_8, $\mathrm{PSL}_3(4)$, $\mathrm{SU}_4(2)$, $\mathrm{PSp}_4(7)$, $\mathrm{PSL}_2(23)$, $\mathrm{PSL}_2(25)$, $\mathrm{PSL}_2(47)$, or $\mathrm{PSL}_2(49)$. In all of these cases, the 2-rank of $\mathrm{Aut}(S)$ is less than 11, see [ATLAS], a contradiction.
- $L = \mathsf{A}_{25}$. Recalling that $\mathbf{Z}(G) \leq C_2$ and that $\mathrm{Out}(S) \cong C_2$ in this case, we see that $N/(N \cap \mathbf{Z}(G))$ contains a subgroup $C_{23} < S$ that acts nontrivially on $Q/(Q \cap \mathbf{Z}(G)) \cong C_2^{11}$. This implies that S contains

a subgroup N_1 with $Q_1 := \mathbf{O}_2(N_1) \cong C_2^{11}$ and $N_1/Q_1 \cong C_{23}$ acting irreducibly on Q_1 (considered as an $\mathbb{F}_2$-module). In turn, the latter implies that C_{23} acts fixed-point-freely on $\mathrm{Irr}(Q_1) \smallsetminus \{1_{Q_1}\}$, and so any transitive permutation action of N_1 with nontrivial Q_1-action must be on at least $1 + 23 = 24$ symbols. Now consider the natural action of $N_1 < S \cong \mathsf{A}_{25}$ on 25 letters. This must admit at least one orbit Ω with nontrivial Q_1-action, and so $24 \leq |\Omega| \leq 25$ by the previous assertion. But this is a contradiction, since neither 24 nor 25 divides $|N_1| = 2^{11} \cdot 23$.

- $L = 2.\mathsf{Co}_1$. In this case, since $\mathrm{Out}(S) = 1$ (see [ATLAS]), we conclude that $G = L$, as stated. □

8. Determination of the monodromy groups

Theorem 8.1. *For the lisse sheaf $\mathcal{H}(\psi, 3\times 13)$ on $\mathbb{G}_m/\mathbb{F}_4$, we have $G_{geom} = G_{arith} = 2.\mathsf{Co}_1$ in its unique (up to equivalence) 24-dimensional irreducible representation (as the automorphism group of the Leech lattice).*

Proof. Choose (!) an embedding of $\overline{\mathbb{Q}}_\ell$ into $\mathbb{C}$. We will show that the result follows from Theorem 7.2.

From Lemma 4.7, we have

$$G_{geom} \lhd G_{arith} \subset \mathrm{O}_{24}(\mathbb{C}).$$

Because $\mathcal{H}(\psi, 3 \times 13)$ is geometrically irreducible, G_{geom} (and a fortiori G_{arith}) is an irreducible subgroup of $\mathrm{O}_{24}(\mathbb{C})$. By Theorem 6.1, G_{arith} (and a fortiori G_{geom}) is a finite subgroup. By Theorem 2.4 and Corollary 1.3, G_{geom} (and a fortiori G_{arith}) is tensor indecomposable and primitive.

By Lemma 3.1, the image of the wild inertia group $P(\infty)$ is the Pontrayagin dual of the additive group of the field $\mathbb{F}_2(\mu_{23}) = \mathbb{F}_{2^{11}}$, acting as the direct sum of the 23 characters $\mathcal{L}_{\psi(23\zeta x)}$, indexed by $\zeta \in \mu_{23}$. The group $I(\infty)/P(\infty)$ acts through its cyclic quotient μ_{23}, with a primitive 23$^{\mathrm{rd}}$ root of unity cyclically permuting the $\mathcal{L}_{\psi(23\zeta x)}$. Thus G_{geom} (and a fortiori G_{arith}) contains the required $N = C_2^{11} \rtimes C_{23}$ subgroup. □

Theorem 8.2. *For each of the lisse sheaves $\mathcal{H}(\psi, 4 \times 5)$ and $\mathcal{H}(\psi, 28^\times)$ on $\mathbb{G}_m/\mathbb{F}_9$, we have*

$$G_{geom} = G_{arith} = 6.\mathsf{Suz}$$

in one of its two (up to equivalence) complex conjugate irreducible representations of degree 12.

Proof. In this case, the result follows from Theorem 7.1. Just as in the proof of Theorem 8.1, we see that both G_{geom} and G_{arith} are finite, irreducible, primitive, tensor indecomposable subgroups of $\mathrm{GL}_{12}(\mathbb{C})$.

By Lemma 3.1, the image of the wild inertia group $P(\infty)$ is the Pontrayagin dual of the additive group of the field $\mathbb{F}_3(\mu_{11}) = \mathbb{F}_{3^5}$, acting as the direct sum of the 11 characters $\mathcal{L}_{\psi(11\zeta x)}$, indexed by $\zeta \in \mu_{11}$. The group $I(\infty)/P(\infty)$ acts through its cyclic quotient μ_{11}, with a primitive 11$^{\mathrm{th}}$ root of unity cyclically permuting the $\mathcal{L}_{\psi(11\zeta x)}$. Thus G_{geom} (and a fortiori G_{arith}) contains the required $N = C_3^5 \rtimes C_{11}$ subgroup.

Therefore by Theorem 7.1, the group G_{arith} (and the group G_{geom}) is the group 6.Suz, augmented by some finite group of scalars. If β is a scalar contained in G_{arith}, then 12β is its trace in the given 12-dimensional representation of G_{arith}. But the traces of G_{arith} lie in $\mathbb{Q}(\zeta_3)$, and thus β lies in $\mathbb{Q}(\zeta_3)$. But β is a root of unity, hence lies in μ_6. But μ_6 lies in 6.Suz, and thus G_{arith} is 6.Suz, and a fortiori G_{geom}, which contains "fewer" scalars, is also 6.Suz. □

Remark 8.3. To see that 2.Co_1 actually contains $C_2^{11} \rtimes C_{23}$, note that 2.Co_1 contains $C_2^{12} \rtimes M_{24} > C_2^{12} \rtimes C_{23}$, see [ATLAS]. Next, as a C_{23}-module, C_2^{12} is semisimple with a 1-dimensional fixed point subspace, leading to the decomposition $C_2^{12} \rtimes C_{23} = (C_2^{11} \rtimes C_{23}) \times C_2$. The same argument, using a maximal subgroup $C_3^5 \rtimes C_{11}$ of Suz [ATLAS] shows that the full inverse image of this subgroup in 6.Suz splits as $(C_3^5 \rtimes C_{11}) \times C_6$, and so 6.$\mathsf{Suz}$ contains $C_3^5 \rtimes C_{11}$.

9. Pullback to $\mathbb{A}^1$

We begin by stating the simple (and well known) lemma that underlies the constructions of this section.

Lemma 9.1. *Let $\mathcal{H}$ be a local system of $\mathbb{G}_m/\mathbb{F}_q$ whose local monodromy at 0 is of finite order M prime to p. For N any prime to p multiple of M, consider the pullback local system*

$$\mathcal{G}(N) := [N]^\star \mathcal{H} := [x \mapsto x^N]^\star \mathcal{H}$$

on $\mathbb{G}_m/\mathbb{F}_q$. Then we have the following results.

(i) *The local system $\mathcal{G}(N)$ on $\mathbb{G}_m/\mathbb{F}_q$ has a unique extension to a local system on $\mathbb{A}^1/\mathbb{F}_q$, call it $\mathcal{G}_0(N)$.*

(ii) *The local systems $\mathcal{G}(N)$ on $\mathbb{G}_m/\mathbb{F}_q$ and $\mathcal{G}_0(N)$ on $\mathbb{A}^1/\mathbb{F}_q$ have the same G_{arith} as each other, and the same G_{geom} as each other.*

(iii) *We have inclusions*

$$G_{arith,\mathcal{G}(N)} < G_{arith,\mathcal{H}}, \quad G_{geom,\mathcal{G}(N)} \lhd G_{geom,\mathcal{H}},$$

and the quotient

$$G_{geom,\mathcal{H}}/G_{geom,\mathcal{G}(N)}$$

is a cyclic group of order dividing N.

Proof. (i) If such an extension exists, it must be $j_\star\mathcal{G}(N)$ for $j : \mathbb{G}_m \subset \mathbb{A}^1$ the inclusion. This direct image is lisse at 0 precisely because the local monodromy of $\mathcal{G}(N)$ at 0 is trivial. (ii) is simply the fact that G_{geom} and G_{arith} are birational invariants. (iii) is Galois theory, and the fact that the extension $\overline{\mathbb{F}_q}(x^{1/N})/\overline{\mathbb{F}_q}(x)$ is Galois, with cyclic Galois group $\mu_N(\overline{\mathbb{F}_q})$. □

Theorem 9.2. *We have the following results.*

(i) *The pullback local system $[39]^\star\mathcal{H}(\psi, 3\times 13)$ on $\mathbb{A}^1/\mathbb{F}_4$ has $G_{geom} = G_{arith} = 2.\mathsf{Co}_1$.*

(ii) *The pullback local system $[20]^\star\mathcal{H}(\psi, 4\times 5)$ on $\mathbb{A}^1/\mathbb{F}_9$ has $G_{geom} = G_{arith} = 6.\mathsf{Suz}$.*

(iii) *The pullback local system $[28]^\star\mathcal{H}(\psi, 28^\times)$ on $\mathbb{A}^1/\mathbb{F}_9$ has $G_{geom} = G_{arith} = 6.\mathsf{Suz}$.*

Proof. For G either of the groups $6.\mathsf{Suz}$ or $2.\mathsf{Co}_1$, G is a perfect group, and hence contains no proper normal subgroup $H \lhd G$ for which G/H is abelian. So in each case listed, it results from Lemma 9.1(iii) above that G_{geom} remains unchanged, equal to G, when we pass from $\mathcal{H}$ to its pullback $\mathcal{G}(N)$. From the inclusion $G_{arith,\mathcal{G}(N)} < G_{arith,\mathcal{H}}$, we have the a priori inclusion $G_{arith,\mathcal{G}(N)} < G$. Thus we have

$$G = G_{geom,\mathcal{G}(N)} \lhd G_{arith,\mathcal{G}(N)} < G.$$

□

Remark 9.3. Although the hypergeometric sheaves in question are rigid local systems on $\mathbb{G}_m$, we do not see any reason their pullbacks to $\mathbb{A}^1$ need be rigid local systems on $\mathbb{A}^1$.

10. Appendix: Another approach to tensor indecomposability

Proposition 10.1. *Let V be a representation of I which is the direct sum $T \oplus W$ of a nonzero tame representation T (i.e., one on which P acts trivially) and of an irreducible representation W which is totally wild (i.e., one in which P has no nonzero invariants). Then V is linearly tensor indecomposable as a representation of I: there do not exist representations V_1 and V_2 of I, each of dimension ≥ 2 and an isomorphism of representations $V_1 \otimes V_2 \cong V$ under each of the three following hypotheses.*

(i) $\dim(V)$ *is not* 4.

(ii) $\dim(V) = 4$, *p odd, and* $\dim(T) \neq 2$.

(iii) $\dim(V) = 4$, *$p = 2$, and* $\dim(T) \neq 1$

Proof. We argue by contradiction, assuming we have $V_1 \otimes V_2 \cong V$. Replacing each of V_1, V_2, V by its semisimplification, we may further assume each is I-semisimple. As P is normal in I (or because the image of P in any continuous ℓ-adic representation is finite), each of these representations is P-semisimple as well.

We have canonical decompositions V_1 and V_2 into direct sums

$$V_1 = T_1 \oplus W_1, \quad V_2 = T_2 \oplus W_2,$$

where the T_i are tame representations of I, and the W_i are totally wild representations of I.

Step 1. All four of T_1, T_2, W_1, W_2 cannot be nonzero. If they were, then $V_1 \otimes V_2$ would contain the sum of $T_1 \otimes W_2$ and $T_2 \otimes W_1$, each of which is a nonzero totally wild representation of I, contradicting that W is irreducible.

Step 2. We cannot have $V_1 = T_1$. For then the wild part W of V is $T_1 \otimes W_2$, so by irreducibility of W the dimension of $V_1 = T_1$ is 1.

Step 3. We cannot have $V_1 = W_1$ and T_2 nonzero. In this case, we would have

$$T \oplus W \cong T_2 \otimes W_1 \oplus W_1 \otimes W_2.$$

From the irreduciblility of W, we see that $\dim(T_2)$ must be 1, and that $W_1 \otimes W_2$ must be entirely tame.

Step 4. Thus we must have $V_1 = W_1$ and $V_2 = W_2$. Write each of W_1, W_2 as a sum of I-irreducibles, say

$$W_1 = \sum_i W_{1,i}, \quad W_2 = \sum_j W_{2,j}.$$

Then $V_1 \otimes V_2 = W_1 \otimes W_2$ is

$$\sum_{i,j} W_{1,i} \otimes W_{2,j}.$$

Of these $\sum_{i,j} W_{1,i} \otimes W_{2,j}$, precisely one summand fails to be totally tame, for the wild part of $V_1 \otimes V_2$, which is irreducible, is the sum of the wild parts of the $W_{1,i} \otimes W_{2,j}$. We then invoke the following lemma.

Lemma 10.2. *Let W_1 and W_2 be irreducible, totally wild representations of I. If $W_1 \otimes W_2$ is entirely tame, then $\dim(W_1) = \dim(W_2) = 1$ and $W_2^\vee \cong W_1 \otimes (\text{some tame character } \chi)$.*

Proof. Decompose each of the W_i into its P-isotypical components. By [Ka-GKM, 1.14.2], we know that each isotypical component is P-irreducible. Thus as P-representations, we have

$$W_1 = \sum_i N_i, \quad W_2 = \sum_j M_j,$$

with the N_i and the M_j each P-irreducible. Then $W_1 \otimes W_2$ is $\sum_{i,j} N_i \otimes M_j$. In the tensor product $N_i \otimes M_j$ of two irreducible representations, the trivial representation occurs either not at all, or just once, and it occurs precisely when $M_j \cong N_i^\vee$. To say that $W_1 \otimes W_2$ is entirely tame is to say that each $N_i \otimes M_j$ is entirely trivial as P-representation, or in other words that each $N_i \otimes M_j$ is both one-dimensional and trivial. For this to hold, each N_i and each M_j has dimension 1, and $M_j \cong N_i^\vee$. for every pair (i, j). Thus all the M_j are isomorphic, each being $N_1^\vee$. Similarly, all the N_i are isomorphic, each being $M_1^\vee$. But the various P-isotypical components of a given irreducible W_i are pairwise nonisomorphic. Thus $W_1 = N_1$ and $W_2 = M_2$ are one-dimensional duals on P, so duals up to tensoring by a tame character on I. $\square$

Returning to our situation

$$V_1 \otimes V_2 = \sum_{i,j} W_{1,i} \otimes W_{2,j},$$

we may renumber so that $W_{1,1} \otimes W_{2,1}$ is not totally tame, but all other $W_{1,i} \otimes W_{2,j}$ are totally tame.

Suppose now that W_1 is the sum of two or more irreducibles, then $V_1 \otimes V_2$ contains

$$(W_{1,1} + W_{1,2}) \otimes W_{2,1},$$

and hence $W_{1,2} \otimes W_{2,1}$ is totally tame. By the above Lemma 10.2, $W_{2,1}$ is one dimensional, and

$$W_{2,1} \cong W_{1,2}^\vee \otimes (\text{some tame character } \chi).$$

If W_2 is the sum of two or more irreducibles, then each product $W_{1,2}) \otimes W_{2,j}$ must be totally tame, hence we have

$$W_{2,j} \cong W_{2,1}^\vee \otimes (\text{some tame character } \chi_j).$$

Thus W_2 is of the form

$$W_2 = (\text{tame } \mathsf{Tame}_2, \dim \geq 1) \otimes \mathrm{W}_{2,1},$$

and $V_1 \otimes V_2$ contains

$$(W_{1,1} + W_{1,2}) \otimes (\mathsf{Tame}_2 \otimes W_{2,1}).$$

In particular $V_1 \otimes V_2$ contains $\dim(\mathsf{Tame}_2)$ pieces of the form

$$W_{1,1} \otimes W_{2,1} \otimes (\text{some tame character}),$$

none of which is totally tame. Therefore Tame_2 is one-dimensional, hence W_2 is one-dimensional, i.e., V_2 is one-dimensional, contradiction.

Thus W_1 is a single irreducible. Repeating the argument with W_1 and W_2 interchanged, W_2 must also be a single irreducible. If $W_1 \otimes W_2$ has a nonzero tame part, say contains a tame character χ, then $W_1 \otimes W_2 \otimes \overline{\chi}$ contains $\mathbb{1}$, and hence

$$W_2 \cong W_1^\vee \otimes \chi.$$

But $W_1 \otimes W_2$ also has a nonzero (in fact irreducible) wild part, hence $\dim(W_1) \geq 2$ (otherwise $W_1 \otimes W_2$ will be χ alone). Thus $\dim(V_1) = \dim(V_2) = \dim(W_1)$, and $\dim(V)$ is a square.

We now examine the situation in which $\dim(V)$ is a square n^2. Thus

$$V \cong W_1 \otimes W_2 = \mathrm{End}(W_1) \otimes \chi,$$

i.e.,

$$V \otimes \overline{\chi} \cong \mathrm{End}(W_1).$$

Now $V \otimes \overline{\chi}$ is itself the sum of a nonzero tame part and an irreducible totally wild part, and $\dim(W_1) = n$. So the question becomes, when is it possible that for a W of dimension n, $\mathrm{End}(W)$ is the sum of a nonzero tame part and an irreducible totally wild part. Let us refer to this as "the End situation". This is the situation we would like to rule out.

We first show that if n is prime to p, the End situation can only arise when $n = 2$. Denote by $I(n) \lhd I$ the unique open subgroup of index n. Thus $I/I(n) \cong \mu_n$. Then W is the sum of n P-isotypical components N_i, each of which is one dimensional, stable by $I(n)$, and each of which is P-inequivalent to any of its nontrivial multiplicative translates $\mathrm{MultTransl}_\zeta(N_i)$ by nontrivial n'th roots of unity ζ. If we fix one of them, say $N := N_1$, then as P-representation

$$W \cong \oplus_{\zeta \in \mu_n} \mathrm{MultTransl}_\zeta(N),$$

and hence as P-representation

$$\mathrm{End}(W) \cong \bigoplus_{(\zeta_1,\zeta_2) \in \mu_n \times \mu_n} \mathrm{MultTransl}_{\zeta_1}(N) \otimes \mathrm{MultTransl}_{\zeta_2}(N^\vee).$$

Each of these n^2 pieces is $I(n)$-stable. The n "diagonal" summands

$$\mathrm{MultTransl}_\zeta(N) \otimes \mathrm{MultTransl}_\zeta(N^\vee)$$

are P-trivial, and their n-dimensional sum is the tame part of $\mathrm{End}(W_1)$. The remaining $n(n-1)$ summands can be put together into $n-1$ pieces, as follows. Start with the $n-1$ summands

$$N \otimes \mathrm{MultTransl}_{\zeta_1}(N^\vee), \zeta_1 \neq 1.$$

For each, form the sum

$$\bigoplus_{\zeta_2} \mathrm{MultTransl}_{\zeta_2}(N \otimes \mathrm{MultTransl}_{\zeta_1}(N^\vee)).$$

Each of these $n-1$ sums is I-stable and totally wild. [It is the induction from $I(n)$ to I of $N \otimes \mathrm{MultTransl}_{\zeta_1}(N^\vee)$.] Thus we have at least $n-1$ totally wild constituents in $V \otimes \overline{\chi}$. But its wild part is irreducible, which is only possible if $n-1 = 1$, i.e., if $n = 2$. In this $n = 2$, the tame part of $\mathrm{End}(W)$ has dimension 2.

We also remark that in this $n = 2$ case, in odd characteristic p, we can indeed have this. Take $W := [2]_\star \mathcal{L}_{\psi(x)}$. Then we have

$$\mathrm{End}(W) = [2]_\star \mathbb{1} + [2]_\star \mathcal{L}_{\psi(2x)} = \mathbb{1} + \chi_2 + [2]_\star \mathcal{L}_{\psi(2x)}.$$

We next show that if $n = n_0 q$ with n_0 prime to p and q a strictly positive power of p, the End situation can only arise if $n_0 = 1$. We argue by contradiction. Suppose, then, that $n_0 > 1$. Denote by $I(n_0) \lhd I$ the unique open subgroup of index n_0. Thus $I/I(n_0) \cong \mu_{n_0}$. Then W is the sum of n_0 P-isotypical components N_i, each of which is q- dimensional, P-irreducible, stable by $I(n_0)$, and each of which is P-inequivalent to any of its nontrivial multiplicative translates $\mathrm{MultTransl}_\zeta(N_i)$ by nontrivial n_0'th roots of unity ζ. If we fix one of them, say $N := N_1$, then as P-representation

$$W \cong \oplus_{\zeta \in \mu_{n_0}} \mathrm{MultTransl}_\zeta(N),$$

and hence as P-representation

$$\mathrm{End}(W) \cong \bigoplus_{(\zeta_1,\zeta_2)\in\mu_{n_0}\times\mu_{n_0}} \mathrm{MultTransl}_{\zeta_1}(N)\otimes\mathrm{MultTransl}_{\zeta_2}(N^\vee).$$

Each of these n_0^2 pieces is $I(n_0)$-stable.

If $\zeta_1=\zeta_2$, the piece

$$\mathrm{MultTransl}_{\zeta_1}(N)\otimes\mathrm{MultTransl}_{\zeta_2}(N^\vee) =$$

$$= \mathrm{MultTransl}_{\zeta_1}(N\otimes N^\vee)$$

is the direct sum of a single tame character with a totally wild part of dimension q^2-1 (simply because N is P-irreducible). If If $\zeta_1\neq\zeta_2$, the piece

$$\mathrm{MultTransl}_{\zeta_1}(N)\otimes\mathrm{MultTransl}_{\zeta_2}(N^\vee)$$

is totally wild, of dimension q^2. Assembling these n_0^2 pieces into n_0 I-stable pieces as in the discussion of the prime to p case, we get n_0 I-stable summands, each of which has a nonzero totally wild piece. But the totally wild part of $\mathrm{End}(W)$ is irreducible, contradiction.

Now we analyze the End situation when $n=q$ is a strictly positive power of p. Thus W is I irreducible of rank q. By [Ka-GKM, 1.14.2], W is P-irreducible. Therefore the space $\mathrm{End}(W)^P$ of P-invariants in $\mathrm{End}(W)$ is one-dimensional, which is to say that $\mathrm{End}(W)$ is the sum of a one-dimensional tame part and a totally wild part of dimension q^2-1. We must show that this totally wild part of dimension q^2-1 cannot be I-irreducible, so long as $q\neq 2$. Equivalently, we must show that the action of I on W cannot have fourth moment 2. For this, we need the following lemma.

Lemma 10.3. *Let W be an irreducible I-representation of dimension q whose fourth moment is 2, equivalently such that $\mathrm{End}(W)$ is the sum $\mathbb{1}+\mathrm{Irred}$. Then there exists a continuous character $\chi: I\to\overline{\mathbb{Q}_\ell}^\times$ such that $\det(W\otimes\chi)$ is a character of finite order. For any such χ, the action of I on $W\otimes\chi$ factors through a finite quotient of I.*

Proof. By the trick of [Ka-S, 9.6.7], any continuous character $\rho: I\to\overline{\mathbb{Q}_\ell}^\times$ has a q'th root, up to a character of finite order: given ρ, we can find a continuous character χ such that χ^q/ρ is a character of finite order. Taking ρ to be $\det(W)$, we get the asserted χ.

Replacing W by $W\otimes\chi$ does not change the fourth moment (indeed it does not change End). So it suffices to treat the case when W has a determinant of finite order.

Denote by G the Zariski closure in $\mathrm{GL}(W)$ of the image of I, and by G_0 the Zariski closure in $\mathrm{GL}(W)$ of the image of P. Thus G is an irreducible (and hence reductive) subgroup of $GL(W)$, with fourth moment 2. Because P is a pro-p group, its image in the ℓ-adic representation is finite. Thus G_0 is finite, and $G_0\lhd G$ (simply because $P\lhd I$). Because the dimension is q, W is P-irreducible. Thus G contains a normal subgroup which is both irreducible and finite. By Larsen's Alternative, cf. [Ka-LAMM, 1.1.6, (2)] or [GT1, Thm. 1.1], either G is finite (the determinant being of finite order forces $G\cap$scalars to be finite) or $G^0=\mathrm{SL}(W)<G<\mathrm{GL}(W)$. This second case cannot occur, because the only normal subgroups of such a G are subgroups of the center, none of which is irreduclble. ◻

With this lemma at hand, we are reduced to considering the following situation. W is an irreducible I-representation of dimension q on which I acts through a finite quotient, such that the fourth moment is 2. Any finite quotient of I is is a finite group Γ with a p-group subgroup $\Gamma_0\lhd\Gamma$ such that Γ/Γ_0 is cyclic of order prime to p. Thus Γ is solvable, and any subgroup $H<\Gamma$ whose order $\#H$ is prime to p is cyclic.

We now compare this information on our Γ with the classification of finite groups with fourth moment 2 given in [BNRT]. More precisely, we use the consequence isolated in Theorem 2.3, which tells us immediately that when the dimension q is a power of an odd prime, the fourth moment of our Γ cannot be 2. When q even but $q\neq 2$, Theorem 2.3 tells us that the solvability of Γ forces its fourth moment to be ≥ 3.

In the case $q=2$, we have the possibility that $\mathrm{End}(W)$ is the sum $\mathbb{1}+\mathrm{Irred}_3$. Indeed, this can happen, cf. [Ka-CC, Cor.3.2]. ◻

Corollary 10.4. *Let V be a representation of I which is the direct sum $T \oplus W$ of a nonzero tame representation T (i.e., one on which P acts trivially) and of an irreducible representation W which is totally wild (i.e., one in which P has no nonzero invariants). Then I stabilizes no decomposition $V = A \otimes B$ with $\dim(A), \dim(B) > 1$ under each of the following three hypotheses.*

(i) $\dim(V)$ *is not* 4.
(ii) $\dim(V) = 4$, *p odd, and* $\dim(T) \neq 2$.
(iii) $\dim(V) = 4$, $p = 2$, *and* $\dim(T) \neq 1$.

Proof. Suppose that I stabilizes such a decomposition $V = A \otimes B$. This means that $\rho(I)$ lies in the subgroup $\mathrm{GL}(A) \otimes \mathrm{GL}(B)$ of $\mathrm{GL}(A \otimes B)$. Observe that an element $a \otimes b \in \mathrm{GL}(A) \otimes \mathrm{GL}(B)$ is equal, for any nonzero scalar λ, to the element $(\lambda a) \otimes (\lambda^{-1} b)$. This allows us to move a to lie in $\mathrm{SL}(A)$. Thus we have an equality of subgroups of $\mathrm{GL}(A \otimes B)$,

$$\mathrm{SL}(A) \otimes \mathrm{GL}(B) = \mathrm{GL}(A) \otimes \mathrm{GL}(B).$$

We have an exact sequence

$$1 \to \mu_{\dim(A)} \to \mathrm{SL}(A) \times \mathrm{GL}(B) \to \mathrm{GL}(A \otimes B) \to 1,$$

the first map being $\zeta \mapsto (\zeta, 1/\zeta)$.

The group I has cohomological dimension ≤ 1, cf. [Serre, Chapter II, 3.3, c)], therefore we have

$$H^2(I, \mu_{\dim(A)}) = 0,$$

and the representation ρ lifts to a representation

$$\overline{\rho} : I \to \mathrm{SL}(A) \times \mathrm{GL}(B),$$

which makes each of A, B into representations of I for which $V \cong A \otimes B$ is an isomorphism of I-representations. Now apply the previous Proposition 10.1. $\square$

References

[BNRT] Bannai E., Navarro, G., Rizo, N., and Tiep, P. H., Unitary t-groups, *J. Math. Soc. Japan* (to appear), arXiv:1810.02507.

[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.

[GAP] The GAP group, GAP - groups, algorithms, and programming, Version 4.4, 2004, http://www.gap-system.org.

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

[GT1] Guralnick, R.M., and Tiep, P.H., Decompositions of small tensor powers and Larsen's conjecture, *Represent. Theory* **9** (2005), 138–208.

[GT2] Guralnick, R. M. and Tiep, P. H., Symmetric powers and a problem of Kollár 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.

[Is] I. M. Isaacs, Character theory of finite groups, AMS-Chelsea, Providence, 2006.

[Ka-CC] Katz, N.. From Clausen to Carlitz: low-dimensional spin groups and identities among character sums, *Mosc. Math. J.* **9** (2009), 57–89.

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

[Ka-GKM] Katz, N., Gauss sums, Kloosterman sums, and monodromy groups, Annals of Mathematics Studies, **116**, Princeton University Press, Princeton, NJ, 1988. x+246 pp.

[Ka-LAMM] Katz, N. Larsen's alternative, moments, and the monodromy of Lefschetz pencils. Contributions to automorphic forms, geometry, and number theory, 521–560, Johns Hopkins Univ. Press, Baltimore, MD, 2004.

[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-RL-T-Co3] Katz, N., Rojas-León, A., and Tiep, P.H., Rigid local systems with monodromy group the Conway group Co_3, *J. Number Theory* (to appear), arXiv:1810.04587.

[Ka-RL-T-Co2] Katz, N., Rojas-León, A., and Tiep, P.H., Rigid local systems with monodromy group the Conway group Co_2, *Int. J. Number Theory* (to appear), arXiv:1811.05712.

[Ka-S] Katz, N. and Sarnak, P., Random matrices, Frobenius eigenvalues, and monodromy. American Mathematical Society Colloquium Publications, **45**. American Mathematical Society, Providence, RI, 1999. xii+419 pp.

[Ka-T] Katz, N. and Tiep, P.H., Monodromy groups of certain Kloosterman and hypergeometric sheaves, (in preparation).

[Kub] Kubert, D., Lectures at Princeton University, May 1986.

[M] Malle, G., Almost irreducible tensor squares, *Comm. Algebra* **27** (1999), 1033–1051.

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

[Serre] Serre, J.P., Cohomologie Galoisienne, 5 éd, rév. et complétée, Springer Lecture Notes in Mathematcs **5**, second printing, 1997.

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`