LOCAL SYSTEMS AND SUZUKI GROUPS

LEVENT ALPÖGE, NICHOLAS M. KATZ, GABRIEL NAVARRO, E.A. O'BRIEN, AND PHAM HUU TIEP

ABSTRACT. We study geometric monodromy groups $G_{\mathrm{geom},\mathcal{F}_q}$ of the local sheaves $\mathcal{F}_q$ on the affine line over $\mathbb{F}_2$ of rank $D = \sqrt{q}(q-1)$, $q = 2^{2n+1}$, constructed in [Ka5]. The main result of the paper shows that $G_{\mathrm{geom},\mathcal{F}_q}$ is either the Suzuki simple group ${}^2B_2(q)$, or the special linear group SL_D. We also show that $\mathcal{F}_8$ has geometric monodromy group ${}^2B_2(8)$, and arithmetic monodromy group $\mathrm{Aut}({}^2B_2(8))$ over $\mathbb{F}_2$, thus establishing [Ka5, Conjecture 2.2] in full in the case $q = 8$.

CONTENTS

INTRODUCTION

In an earlier paper [Ka5], one of us, inspired by a paper [Gr] of Gross, defined, for each $n \geq 1$, a local system on $\mathbb{A}^1/\mathbb{F}_2$ of rank $2^n(2^{2n+1}-1)$, whose geometric monodromy group we conjectured to

2010 *Mathematics Subject Classification.* Primary 11T23, Secondary 20C15, 20C33, 20D06, 20G05.

Key words and phrases. Local systems, Airy sheaves, Monodromy groups, Suzuki simple groups.

The first author gratefully acknowledges the support of the NSF (grant DMS-2002109) and the Society of Fellows.

The third author gratefully acknowledges the support of the Grant PID2019-103854GB-I00 funded by MCIN/AEI-/10.13039/501100011033.

The fourth author gratefully acknowledges the support of the Marsden Fund of New Zealand via grant UOA 107.

The fifth author gratefully acknowledges the support of the NSF (grants DMS-1840702 and DMS-2200850), the Simons Foundation, and the Joshua Barlaz Chair in Mathematics.

The authors are grateful to the referee for careful reading and helpful comments on the paper.

be the Suzuki group $\mathrm{Sz}(q) := {}^2B_2(q),\ q = 2^{2n+1}$, in one of its two lowest dimensional nontrivial irreducible representations. These representations, complex conjugates of each other, are of dimension $2^n(2^{2n+1}-1)$ and have traces in $\mathbb{Z}[i]$, the Gaussian integers.

The definition involved p-Witt vectors of length 2 for $p = 2$, with values in $\mathbb{F}_2$-algebras. We identify $W_2(\mathbb{F}_2)$ with $\mathbb{Z}/4\mathbb{Z}$, by the map $[a,b] \mapsto a^2 + 2b$, with the usual convention that we first lift a, b to $\mathbb{Z}$ and then reduce $a^2 + 2b$ modulo 4. We take the additive character of $\mathbb{Z}/4\mathbb{Z}$ given by $n \mapsto i^n$, and view it as the additive character $\psi_2 : W_2(\mathbb{F}_2) \to \mu_4(\mathbb{Z}[i])$ given by

$$\psi_2([a,b]) := i^{a^2+2b}.$$

Attached to a Witt vector of length 2 with coefficients in $\mathbb{F}_2[x]$, say $[a(x), b(x)]$, is the Artin-Schreier-Witt sheaf $\mathcal{L}_{\psi_2([a(x),b(x)])}$ on $\mathbb{A}^1/\mathbb{F}_2$. It is lisse of rank one, and its trace function is given as follows. For $k/\mathbb{F}_2$ a finite extension, and $x \in k$,

$$\mathrm{Trace}(\mathrm{Frob}_{x,k}|\mathcal{L}_{\psi_2([a(x),b(x)])}) = \psi_2(\mathrm{Trace}_{W_2(k)/W_2(\mathbb{F}_2)}([a(x),b(x)]).$$

If instead we take $a(x), b(x) \in k_0[x]$ for some finite extension $k_0/\mathbb{F}_2$, then the Artin-Schreier-Witt sheaf $\mathcal{L}_{\psi_2([a(x),b(x)])}$ is lisse of rank one on $\mathbb{A}^1/k_0$, and for k/k_0 a finite extension and $x \in k$, the trace of $\mathrm{Frob}_{x,k}$ is given by the same formula (which only makes sense when k is an extension of k_0).

The unique nontrivial additive character ψ of $\mathbb{F}_2$ is related to ψ_2 by the formula

$$\psi(b) = \psi_2([0,b]);$$

this is simply the identity $(-1)^b = i^{2b}$.

Under Witt vector addition, $[a,b] = [a,0] + [0,b]$. Thus we have the factorization

$$\mathcal{L}_{\psi_2([a(x),b(x)])} = \mathcal{L}_{\psi_2([a(x),0])} \otimes \mathcal{L}_{\psi(b(x))}.$$

When both $a(x)$ and $b(x)$ are polynomials of degree prime to $p = 2$, $\mathcal{L}_{\psi_2([a(x),0])}$ has Swan conductor $\mathsf{Swan}_\infty = p\deg(a(x))$, while $\mathcal{L}_{\psi(b(x))}$ has $\mathsf{Swan}_\infty = \deg(b(x))$. So in this case, $\mathcal{L}_{\psi_2([a(x),b(x)])}$ has $\mathsf{Swan}_\infty = \max(p\deg(a(x)), \deg(b(x)))$.

Quite generally, for an Artin-Schreier-Witt sheaf $\mathcal{L} := \mathcal{L}_{\psi_2([a(x),b(x)])}$ on $\mathbb{A}^1/k_0$ with Swan conductor $\mathsf{Swan}_\infty = n \geq 2$, its Fourier transform $\mathrm{FT}_\psi(\mathcal{L})$ on $\mathbb{A}^1/k_0$ is an *Airy sheaf* in the sense of Šuch [Such]. It is lisse of rank $n-1$, and all its ∞-slopes are $\frac{n}{n-1}$. It is pure of weight one. Its trace function is given as follows: for k/k_0 a finite extension, and $t \in k$,

$$\mathrm{Trace}(\mathrm{Frob}_{t,k}|\mathrm{FT}_\psi(\mathcal{L})) = -\sum_{x\in k} \psi_2\big(\mathrm{Trace}_{W_2(k)/W_2(\mathbb{F}_2)}([a(x), b(x)+tx])\big).$$

Some key facts about Airy sheaves and their monodromy groups are due to Šuch [Such], and are fundamental for the investigations reported on here.

We now turn to the Suzuki "candidates" of [Ka5]. Here

$$n \geq 1\ , q_0 := 2^n,\ q := 2q_0^2,\ t(q) := q + 1 - 2q_0.$$

We take the Witt vector

$$[x^{t(q)}, \sum_{i=1}^{n} x^{(1+2^i)t(q)}],$$

form the Artin-Schreier-Witt sheaf

$$\mathcal{L} := \mathcal{L}_{\psi_2([x^{t(q)}, \sum_{i=1}^n x^{(1+2^i)t(q)}])},$$

form its $\mathrm{FT}_\psi(\mathcal{L})$, and twist by the constant field twist $(\frac{1}{1-(-1)^n\, i})^{\deg}$, to arrive at the local system $\mathcal{F}_q$ on $\mathbb{A}^1/\mathbb{F}_2$, whose trace function is given as follows. For $k/\mathbb{F}_2$ a finite extension, and $t \in k$,

$$\mathrm{Trace}(\mathrm{Frob}_{t,k}|\mathcal{F}_q) = \frac{-1}{\big(1-(-1)^n\, i\big)^{\deg(k/\mathbb{F}_2)}} \sum_{x\in k} \psi_2\big(\mathrm{Trace}_{W_2(k)/W_2(\mathbb{F}_2)}([x^{t(q)}, \sum_{i=1}^{n} x^{(1+2^i)t(q)} + tx])\big).$$

A key fact about $\mathcal{F}_q$ is that the input Witt vector $[x^{t(q)}, \sum_{i=1}^{n} x^{(1+2^i)t(q)}]$ is a function of $x^{t(q)}$. So in the trace formula for $\mathcal{F}_q$, if we restrict to $t \neq 0$ and make the substitution $x \mapsto x/t$, the formula becomes

$$\mathrm{Trace}(\mathrm{Frob}_{t,k}|\mathcal{F}_q) = \frac{-1}{\big(1-(-1)^n\, i\big)^{\deg(k/\mathbb{F}_2)}} \sum_{x\in k} \psi_2\big(\mathrm{Trace}_{W_2(k)/W_2(\mathbb{F}_2)}([\frac{x^{t(q)}}{t^{t(q)}}, \sum_{i=1}^{n} \frac{x^{(1+2^i)t(q)}}{t^{(1+2^i)t(q)}} + x])\big),$$

which is a function of $t^{t(q)}$. Thus $\mathcal{F}_q|\mathbb{G}_m$ has a descent to a lisse sheaf $\mathcal{G}_q$ on $\mathbb{G}_m/\mathbb{F}_2$ whose trace function is given by

$$\mathrm{Trace}(\mathrm{Frob}_{t,k}|\mathcal{F}_q) = \frac{-1}{\big(1-(-1)^n\, i\big)^{\deg(k/\mathbb{F}_2)}} \sum_{x\in k} \psi_2\big(\mathrm{Trace}_{W_2(k)/W_2(\mathbb{F}_2)}([\frac{x^{t(q)}}{t}, \sum_{i=1}^{n} \frac{x^{(1+2^i)t(q)}}{t^{(1+2^i)}} + x])\big),$$

and such that under the $t(q)$ Kummer pullback,

$$[t(q)]^\star \mathcal{G}_q = \mathcal{F}_q|\mathbb{G}_m.$$

For the case $n = 1$, i.e. for ${}^2B_2(8)$, we prove in Theorem 6.1 that $\mathcal{F}_8$ has the predicted geometric monodromy group $G_{\mathrm{geom},\mathcal{F}_8} = {}^2B_2(8)$ and arithmetic monodromy group $G_{\mathrm{arith},\mathcal{F}_8,\mathbb{F}_2} = \mathrm{Aut}({}^2B_2(8))$ over $\mathbb{F}_2$, and thus establish [Ka5, Conjecture 2.2] in full in this case. For each $n \geq 1$, we show that $G_{\mathrm{geom},\mathcal{F}_q}$ is either ${}^2B_2(q)$ or SL_D for $D = \mathrm{rank}(\mathcal{F}_q) = q_0(q-1)$. A (huge) calculation of fourth moment for $\mathcal{F}_8$ shows that $G_{\mathrm{geom},\mathcal{F}_8}$ cannot be SL_{14}. It remains an open problem to prove (or disprove) that each $\mathcal{F}_q$ has $G_{\mathrm{geom},\mathcal{F}_q} = {}^2B_2(q)$ when $q \geq 32$.

In fact, we show in Theorem 8.4 that we have such a dichotomy of possible geometric monodromy groups G_{geom}, either ${}^2B_2(q)$ or SL_D, $D = q_0(q-1)$, for a general class of local systems of "the same shape" as $\mathcal{F}_q$ (see Remark 8.6 and Theorem 9.18 for examples of such local systems with $G_{\mathrm{geom}} = \mathrm{SL}_D$). Key to our investigation is the fact that these sheaves all satisfy the condition (**S**+) of [KT1, Definition 1.2]. Somewhat to our surprise, the most difficult part of establishing condition (**S**+) was to show the sheaves in question are geometrically primitive, i.e. that the representation of their G_{geom} is not induced. Our proof utilizes the existence of primitive prime divisors of the integer $t(q)$, cf. Theorem 3.4. We give a second proof which will be useful in future studies of geometric monodromy groups of quite general Airy sheaves. Condition (**S**+) implies that for each of these sheaves, either G_{geom} is a finite, almost quasisimple group, or has G°_{geom} acting irreducibly. This initial dichotomy, plus a substantial group-theoretic analysis, in which Theorem 4.5 plays a key role, is what leads to the ${}^2B_2(q)/\mathrm{SL}_D$ dichotomy. Pursuing the study of primitive prime divisors, we prove in Theorems 3.4, 3.7, and Corollary 3.5 the existence of primitive prime divisors in the orders of maximal tori of the Suzuki-Ree groups ${}^2B_2(q)$, ${}^2G_2(q)$, and ${}^2F_4(q)$. We also extend in §7 the classification of low-dimensional representations of classical groups in characteristic $p \geq 0$, beyond the bounds in [KlL] and [Lu]. These results will be useful in other situations as well. Finally, the structure of arithmetic monodromy groups, assuming finiteness, is determined in Theorem 9.14.

1. Descents of Suzuki candidates and moment calculations

For each odd power $q = 2^{2n+1}$ of 2, starting with $q = 8$, the finite simple group ${}^2B_2(q)$ has two (complex conjugate) lowest dimensional nontrivial irreducible representations, of dimension

$d(q) := q_0(q-1)$, with $q_0 := 2^n$. In each case we have a factorization

$$1 + d(q) = (q_0 + 1)t(q) \quad \text{with } t(q) := q + 1 - 2q_0.$$

In [Ka5], for each such q there is proposed an Airy sheaf in the sense of Šuch [Such], call it $\mathcal{F}_q$ on $\mathbb{A}^1/\mathbb{F}_2$ which is lisse of rank $d(q)$ and with $\mathsf{Swan}_\infty(\mathcal{F}_q) = 1 + d(q)$. Its $I(\infty)$-representation is irreducible of dimension $d(q)$, with all ∞-slopes $\frac{1+d(q)}{d(q)}$. Moreover, $\mathcal{F}_q$ is given [Ka5, Section 4] with an explicit descent to a lisse sheaf $\mathcal{G}_q$ on $\mathbb{G}_m/\mathbb{F}_2$ whose Kummer pullback by $t(q)^{\text{th}}$ power is (the restriction to $\mathbb{G}_m/\mathbb{F}_2$ of) $\mathcal{F}_q$:

$$[t(q)]^\star \mathcal{G}_q \cong \mathcal{F}_q | \mathbb{G}_m.$$

Thus $\mathcal{G}_q$ is lisse on $\mathbb{G}_m/\mathbb{F}_2$, tame at 0 with $I(0)$-representation a direct sum of Kummer characters of order dividing $t(q)$, and whose $I(\infty)$-representation is irreducible of dimension $d(q)$, with all ∞-slopes $\frac{q_0+1}{d(q)} = \frac{q_0+1}{q_0(q-1)}$.

Next we give a slight improvement of [KRLT2, Theorem 6.5].

Theorem 1.1. *Let $\mathcal{H}_0$ be a lisse sheaf on $\mathbb{G}_m/\mathbb{F}_q$ which is tame at 0 and pure of weight zero. Let a, b be nonnegative integers, and consider the moment $M_{a,b}$. Denote by*

$$\mathcal{H}_0^{a,b} := \mathcal{H}_0^{\otimes a} \otimes (\mathcal{H}_0^\vee)^{\otimes b}.$$

Denote by A, B, C, D the following constants.

$$C := \text{dimension of the space of } I(0)\text{-invariants in } \mathcal{H}_0^{a,b},$$
$$D := \text{dimension of the space of } I(\infty)\text{-invariants in } \mathcal{H}_0^{a,b},$$
$$B := \mathsf{Swan}_\infty(\mathcal{H}_0^{a,b}) + M_{a,b},$$
$$A := B + M_{a,b} - C - D.$$

Then we have the following estimate.

$$\left| \frac{1}{q-1} \sum_{u \in \mathbb{F}_q^\times} \mathrm{Trace}(\mathrm{Frob}_{u,\mathbb{F}_q} | \mathcal{H}_0^{a,b}) \right| \leq \frac{q}{q-1} M_{a,b} + \frac{A\sqrt{q}}{q-1} + \frac{B-A}{q-1}.$$

Proof. For any lisse sheaf $\mathcal{F}$ on $\mathbb{G}_m$, the Lefschetz trace formula gives

$$\sum_{u \in \mathbb{F}_q^\times} \mathrm{Trace}(\mathrm{Frob}_{u,\mathbb{F}_q} | \mathcal{F}) = \mathrm{Trace}\big(\mathrm{Frob}_{\mathbb{F}_q} | H_c^2(\mathbb{G}_m/\overline{\mathbb{F}_q}, \mathcal{F})\big) - \mathrm{Trace}\big(\mathrm{Frob}_{\mathbb{F}_q} | H_c^1(\mathbb{G}_m/\overline{\mathbb{F}_q}, \mathcal{F})\big).$$

If $\mathcal{F}$ is pure of weight zero, then H_c^2 is pure of weight 2, and H_c^1 is mixed of weight ≤ 1, indeed

$$H_c^1 = H_c^1(\mathrm{wt} = 1) \oplus H_c^1(\mathrm{wt} \leq 0).$$

Thus for $\mathcal{F}$ pure of weight zero,

$$\big| \sum_{u \in \mathbb{F}_q^\times} \mathrm{Trace}(\mathrm{Frob}_{u,\mathbb{F}_q} | \mathcal{F}) \big| \leq q h_c^2 + \sqrt{q} h_c^1(\mathrm{wt} = 1) + h_c^1(\mathrm{wt} \leq 0).$$

When $\mathcal{F}$ is tame at 0, the Euler-Poincaré formula gives

$$\mathsf{Swan}_\infty(\mathcal{F}) = h_c^1 - h_c^2.$$

To compute the dimension of $H_c^1(\mathrm{wt} = 1)$, we use the fact that for the inclusion $j : \mathbb{G}_m \subset \mathbb{P}^1$, the group $H^1(\mathbb{P}^1/\overline{\mathbb{F}_q}, j_\star \mathcal{F})$ is pure of weight one. We exploit this by looking at the short exact sequence of sheaves on $\mathbb{P}^1/\overline{\mathbb{F}_q}$ given by

$$0 \to j_! \mathcal{F} \to j_\star \mathcal{F} \to (\mathcal{F}^{I(0)})_0 \oplus (\mathcal{F}^{I(\infty)})_\infty \to 0,$$

where the last two summands are skyscraper sheaves at 0 and ∞. The group

$$H^2(\mathbb{P}^1/\overline{\mathbb{F}_q}, j_\star\mathcal{F}) = H^2_c(\mathbb{G}_m/\overline{\mathbb{F}_q}, \mathcal{F})$$

is the Tate-twisted group of π_1^{geom} co-invariants in $\mathcal{F}$, but as $\mathcal{F}$ is pure, the action of π_1^{geom} is semisimple, so this is also the (Tate-twisted) group of π_1^{geom} invariants. The group

$$H^0(\mathbb{P}^1/\overline{\mathbb{F}_q}, j_\star\mathcal{F}) = H^0(\mathbb{G}_m/\overline{\mathbb{F}_q}, \mathcal{F})$$

is the space of π_1^{geom} invariants in $\mathcal{F}$, so has dimension $h^0 = h^2_c$. Consider the long exact sequence

$$0 \to H^0(\mathbb{P}^1/\overline{\mathbb{F}_q}, j_\star\mathcal{F}) \to \mathcal{F}^{I(0)} \oplus \mathcal{F}^{I(\infty)} \to H^1_c(\mathbb{G}_m/\overline{\mathbb{F}_q}, \mathcal{F}) \to H^1(\mathbb{P}^1/\overline{\mathbb{F}_q}, j_\star\mathcal{F}_0) \to 0.$$

Apply it with $\mathcal{F}$ taken to be $\mathcal{H}_0^{a,b}$. Then $h^0 = h^2_c$ is $M_{a,b}$, and the Euler-Poincaré formula gives

$$h^1_c = \mathsf{Swan}_\infty(\mathcal{H}_0^{a,b}) + M_{a,b}.$$

Thus we have the equalities

$$h^1_c(\text{wt} = 1) = h^1_c + h^0 - \dim \mathcal{F}^{I(0)} - \dim \mathcal{F}^{I(\infty)} = A,$$

and

$$h^1_c(\text{wt} \le 0) = B - A.$$

Then the estimate

$$|\sum_{u\in\mathbb{F}_q^\times} \text{Trace}(\text{Frob}_{u,\mathbb{F}_q}|\mathcal{F})| \le qh^2_c + \sqrt{q}h^1_c(\text{wt} = 1) + h^1_c(\text{wt} \le 0)$$

becomes

$$\big|\sum_{u\in\mathbb{F}_q^\times} \text{Trace}(\text{Frob}_{u,\mathbb{F}_q}|\mathcal{H}_0^{a,b})\big| \le qM_{a,b} + A\sqrt{q} + (B - A).$$

□

We will now apply this estimate to the descent $\mathcal{G}_8$ to $\mathbb{G}_m/\mathbb{F}_2$ of the lisse sheaf $\mathcal{F}_8$ on $\mathbb{A}^1/\mathbb{F}_2$. Recall from [Ka5, §2] that $\mathcal{F}_8$ is the Fourier transform of the Artin-Schreier-Witt sheaf $\mathcal{L}_{\psi_2([x^5,x^{15}])}$, with a constant field twist by $\frac{1}{1+i}$. Thus for $k/\mathbb{F}_2$ a finite extension, and $t \in k$,

$$\text{Trace}(\text{Frob}_{t,k}|\mathcal{F}_8) = -(\frac{1}{1+i})^{\deg(k/\mathbb{F}_2)} \sum_{x\in k} \psi_2(\text{Trace}_{W_2(k)/W_2(\mathbb{F}_2)}([x^5, x^{15} + tx])).$$

The descent $\mathcal{G}_8$ is the lisse sheaf on $\mathbb{G}_m/\mathbb{F}_2$ whose trace function is given as follows. For $k/\mathbb{F}_2$ a finite extension, and $t \in k^\times$,

$$\text{Trace}(\text{Frob}_{t,k}|\mathcal{G}_8) = -(\frac{1}{1+i})^{\deg(k/\mathbb{F}_2)} \sum_{x\in k} \psi_2(\text{Trace}_{W_2(k)/W_2(\mathbb{F}_2)}([x^5/t, x^{15}/t^3 + x])).$$

Thus one visibly has, for $t \in k^\times$, the identity

$$\text{Trace}(\text{Frob}_{t,k}|\mathcal{F}_8) = \text{Trace}(\text{Frob}_{t^5,k}|\mathcal{G}_8),$$

simply by the substitution $x \mapsto x/t$ in the formula for $\mathcal{F}_8$.

In any extension field $k/\mathbb{F}_2$ such that $\gcd(5, \#k^\times) = 1$, the map $t \mapsto t^5$ is bijective on $k^\times$. Such $k/\mathbb{F}_2$ are precisely those whose degree over $\mathbb{F}_2$ is not divisible by 4. For such a $k/\mathbb{F}_2$, the traces $\text{Trace}(\text{Frob}_{t,k}|\mathcal{G}_8)$ as t runs over $k^\times$ are precisely the traces $\text{Trace}(\text{Frob}_{t,k}|\mathcal{F}_8)$ as t runs over $k^\times$. An extensive calculation shows that over $\mathbb{F}_{2^{18}}^\times$, the seven traces which occur, with their multiplicities, are

- $-2i$, multiplicity 16256,
- -2, multiplicity 4095,

- -1, multiplicity 52429,
- 0, multiplicity 112347,
- 1, multiplicity 60495,
- $2i$, multiplicity 16512,
- 14, multiplicity 9.

[We have not been able to find any conceptual explanation for the multiplicities of these traces, let alone for the fact that all traces are algebraic integers. Had we known that the traces of all Frobenii over all finite extensions of $\mathbb{F}_2$ are algebraic integers, we would have been able to conclude that $\mathcal{G}_8$ has finite geometric monodromy group G_{geom}, and the proof of the main result Theorem 6.1 would have been much simpler.]

This computation was carried out using Magma 2.26-6 [BCP] at the University of Auckland. It exploited a new feature of Magma which supports running tasks in parallel on multiple processors: each task performed the necessary computation for a given $t \in k^\times$. Using 55 3.0GHz processors, the computation completed in 5.75 days, taking about 7500 hours of CPU time.

The empirical $M_{2,2}$ for $\mathcal{G}_8$ over $\mathbb{F}_{2^{18}}^\times$ is thus approximately 3.99963378766551080898593515753. Applying Theorem 1.1, we find

Corollary 1.2. *For the lisse sheaf $\mathcal{G}_8$ on $\mathbb{G}_m/\mathbb{F}_2$, $M_{2,2} > 2$.*

Proof. The sheaf $\mathcal{F}_8$ is a geometrically irreducible Airy sheaf, lisse on $\mathbb{A}^1/\mathbb{F}_2$ of rank 14, whose $I(\infty)$ representation is irreducible, with all slopes 15/14. Its descent $\mathcal{G}_8$ is thus lisse and geometrically irreducible on $\mathbb{G}_m$, its $I(0)$ representation is the direct sum with multiplicities of the characters of order dividing 5, and its $I(\infty)$ representation is irreducible, with all slopes 3/14.

Let us denote by

$$\mathcal{K} := (\mathcal{G}_8)^{\otimes 2} \otimes (\mathcal{G}_8^\vee)^{\otimes 2}.$$

In the proof of Theorem 1.1, the estimate

$$\Big|\sum_{t\in\mathbb{F}_q^\times} \mathrm{Trace}(\mathrm{Frob}_{t,\mathbb{F}_q}|\mathcal{K})\Big| \le q h_c^2 + \sqrt{q} h_c^1(\mathrm{wt}=1) + h_c^1(\mathrm{wt}\le 0)$$

can first be weakened to

$$\Big|\sum_{x\in\mathbb{F}_q^\times} \mathrm{Trace}(\mathrm{Frob}_{u,\mathbb{F}_q}|\mathcal{K})\Big| \le q h_c^2 + \sqrt{q} h_c^1(\mathrm{wt}=1) + h_c^1.$$

The equality

$$h_c^1(\mathrm{wt}=1) = \mathsf{Swan}_\infty(\mathcal{K}) + 2M_{2,2} - \dim \mathcal{K}^{I(0)} - \dim \mathcal{K}^{I(\infty)}$$

can be weakened to

$$h_c^1(\mathrm{wt}=1) \le \mathsf{Swan}_\infty(\mathcal{K}) + M_{2,2} - \dim \mathcal{K}^{I(0)},$$

simply because in the exact sequence, the space H^0 of global invariants of $\mathcal{K}$ injects into the space $\mathcal{K}^{I(\infty)}$ of $I(\infty)$-invariants.

Thus $\mathcal{K}$ is lisse on $\mathbb{G}_m$, its $I(0)$ representation is the direct sum with multiplicities of the characters of order dividing 5, and all its $I(\infty)$ slopes are $\le 3/14$. So we have the crude estimate

$$\mathsf{Swan}_\infty(\mathcal{K}) \le \mathrm{rank}(\mathcal{K})(\text{biggest slope}) \le 14^4(3/14) = 8232.$$

The $I(0)$ representation of $\mathcal{K}$ is End(End(the $I(0)$-representation of $\mathcal{G}_8$)).

We now turn to the $I(0)$ representation of $\mathcal{G}_8$. The action of $I(0)$ is through μ_5. So in terms of a fixed character χ of order 5, it is a direct sum

$$a\mathbb{1} + b\chi + c\chi^2 + d\chi^3 + e\chi^4,$$

with non-negative integers a, b, c, d, e which sum to 14. We also know from Deligne's "independence of ℓ" result [De2, Theorem 9.8] or from Serre-Tate [Se-Ta, Theorem 2(ii)], that the character of this representation of $I(0)$ has values in the field $\mathbb{Q}(i)$ (because $\mathcal{G}_8$ is part of a compatible system over $\mathbb{Q}(i)$). On the other hand, this character has values in $\mathbb{Q}(\zeta_5)$. But the intersection $\mathbb{Q}(i) \cap \mathbb{Q}(\zeta_5)$ is just $\mathbb{Q}$, so the trace has values in $\mathbb{Q}$. In other words, the quantity

$$a + b\zeta_5 + c\zeta_5^2 + d\zeta_5^3 + e\zeta_5^4$$

lies in $\mathbb{Q}$. This in turn forces $b = c = d = e$, and so $a + b\zeta_5 + b\zeta_5^2 + b\zeta_5^3 + b\zeta_5^4 = a - b$. But $a + 4b = 14$, so there are only four possibilities for the character, namely

$$2\mathbb{1} + 3\chi + 3\chi^2 + 3\chi^3 + 3\chi^4,\ , 6\mathbb{1} + 2\chi + 2\chi^2 + 2\chi^3 + 2\chi^4, 10\mathbb{1} + 1\chi + 1\chi^2 + 1\chi^3 + 1\chi^4,\ 14\mathbb{1}.$$

More intrinsically, let us denote by Reg the regular representation of μ_5:

$$\mathsf{Reg} = \mathbb{1} + \chi + \chi^2 + \chi^3 + \chi^4.$$

Then the $I(0)$ representation of $\mathcal{G}_8$ is one of

$$-\mathbb{1} + 3\mathsf{Reg},\ 4\mathbb{1} + 2\mathsf{Reg},\ 9\mathbb{1} + \mathsf{Reg},\ 14\mathbb{1}.$$

Because the character takes real (in fact integer) values, $\dim \mathcal{K}^{I(0)}$ is the coefficient of $\mathbb{1}$ in the fourth power of the character. For each of our four candidates, this is easily computed by hand, because $\mathsf{Reg}^2 = 5\mathsf{Reg}$, $\mathsf{Reg}^3 = 5^2\mathsf{Reg}$, $\mathsf{Reg}^4 = 5^3\mathsf{Reg}$. The least of the possible values of $\dim \mathcal{K}^{I(0)}$ is 7684, the value attained by the candidate $-\mathbb{1} + 3\mathsf{Reg}$. So the weakened estimate becomes

$$\Big|\sum_{t \in \mathbb{F}_{2^{18}}^\times} \mathrm{Trace}(\mathrm{Frob}_{t,\mathbb{F}_{2^{18}}}|\mathcal{K})\Big| \le 2^{18}M_{2,2} + (8232 + M_{2,2} - 7684)2^9 + (8232 + M_{2,2}).$$

Dividing by $2^{18} - 1$, we get

$$3.999 \le \frac{2^{18}}{2^{18}-1}M_{2,2} + \frac{(548 + M_{2,2})2^9}{2^{18}-1} + \frac{8232 + M_{2,2}}{2^{18}-1}.$$

Here $2^{18} - 1 = 262143$, and $2^9/(2^{18} - 1) \le (2^9 + 1)/(2^{18} - 1) = 1/(2^9 - 1) = 1/511$.

Thus if $M_{2,2}$ were 2, we would get

$$3.999 \le (1 + (1/262143))2 + 550/511 + 8332/262143,$$

which is nonsense. □

2. Background results on determinants, rationality, and slopes

Theorem 2.1. *Let p be a prime, $k/\mathbb{F}_p$ a finite extension, $\nu \ge 1$ an integer, and $\mathcal{F}$ a lisse $\overline{\mathbb{Q}_\ell}$ sheaf on a smooth, geometrically connected scheme U/k which is pure of weight zero and part of a compatible system of lisse sheaves on U whose trace functions take values in $\mathbb{Q}(\zeta_{p^\nu})$. Denote by $G_{\mathrm{geom}} \le G_{\mathrm{arith}}$ the geometric and arithmetic monodromy groups of $\mathcal{F}$. Then we have the following results.*

(i) $\det(G_{\mathrm{arith}})$ *has finite order dividing $2p^\nu$ if p is odd, dividing 2^ν if $p = 2$.*
(ii) $\det(G_{\mathrm{geom}})$ *has finite order dividing $2p^\nu$ if p is odd, dividing 2^ν if $p = 2$.*
(iii) *Suppose that U is a dense open set of $\mathbb{P}^1$, and that at each point $x \in \mathbb{P}^1(\overline{k})\backslash U(\overline{k})$, all $I(x)$-slopes of $\mathcal{F}$ are < 1. Then $\det(G_{\mathrm{geom}})$ has order dividing 2, and is trivial if $p = 2$.*

Proof. (i) For any finite extension L/k and any point $t \in U(L)$, $\det(\mathrm{Frob}_{t,L}|\mathcal{F})$ lies in $\mathbb{Q}(\zeta_{p^\nu})$. It has absolute value 1 at every archimedean place of $\mathbb{Q}(\zeta_{p^\nu})$ (purity of weight zero), and is a λ-adic unit at every finite place λ of residue characteristic $\ne p$ (being part of a compatible system). Because $\mathbb{Q}(\zeta_{p^\nu})$ has a unique place above p, the product formula tells us that this determinant is a unit at

all finite places. Thus it is a root of unity in $\mathbb{Q}(\zeta_{p^\nu})$, so of order dividing $2p^\nu$ for p odd, and of order dividing 2^ν if $p = 2$.

As G_{geom} is a subgroup of G_{arith}, we trivially obtain (ii).

To prove (iii), the slope hypotheses imply that det as a character of G_{geom} has slope < 1, hence 0, at each missing point, and thus is everywhere tame, and hence (being on a dense open set of $\mathbb{P}^1$) has order prime to p. □

Theorem 2.2. *Let p be a prime, $k/\mathbb{F}_p$ a finite extension, $\nu \geq 1$ an integer, and $\mathcal{F}$ a lisse $\overline{\mathbb{Q}_\ell}$ sheaf on a smooth, geometrically connected scheme U/k which is pure of weight zero and part of a compatible system of lisse sheaves on U whose trace functions take values in a number field E. Suppose further that there exists a proper smooth curve with geometrically connected fibres*

$$\pi : \mathcal{C} \to U,$$

a finite group Γ of automorphisms of $\mathcal{C}/U$, and a linear character

$$\chi : \Gamma \to E^\times$$

such $\mathcal{F}$ is isomorphic to the χ-component of $R^1\pi_\star(\overline{\mathbb{Q}_\ell})$. Then we have the following results.

(i) *For any finite extension L/k and any point $t \in U(L)$, the action of $\mathrm{Frob}_{t,L}|\mathcal{F}$ is semisimple.*

(ii) *If U is a curve, with complete nonsingular model X, then for each point $x \in X(\overline{k}) \setminus U(\overline{k})$, the character of the action of the inertia group $I(x)$ acting on $\mathcal{F}$ has values in K.*

Proof. The semisimplicity of Frobenii on H^1 of curves goes back to Weil. By Serre-Tate [Se-Ta, Theorem 2(ii)], the character of $I(x)$ on $R^1\pi_\star(\overline{\mathbb{Q}_\ell})$ has values in $\mathbb{Z}$. When we project the $I(x)$ action onto the χ component, the character of the resulting $I(x)$ action has values in $\mathbb{Q}(\chi)$, a subfield of K. □

Remark 2.3. Theorem 2.2 applies to the Airy sheaves of Šuch [Such] and any of their descents, where the family of curves in question is a family of Artin-Schreier-Witt coverings of $\mathbb{A}^1$ (compactified by adding its one point at ∞).

Next we record a general result on G_{geom} of lisse sheaves on open sets of $\mathbb{A}^1$:

Theorem 2.4. *Let U be a dense open set of $\mathbb{A}^1/\overline{\mathbb{F}_p}$, and $\mathcal{F}$ a lisse $\overline{\mathbb{Q}_\ell}$-sheaf on U, with $\ell \neq p$. Suppose all the ∞-slopes of $\mathcal{F}$ are at most σ, for some $0 < \sigma < 1$. Suppose the geometric monodromy group $G = G_{\text{geom}}$ of $\mathcal{F}$ admits a representation $\Phi : G \to \mathrm{GL}_d(\mathbb{F})$ over some algebraically closed field $\mathbb{F}$ of characteristic $\neq p$, of dimension $d < 1/\sigma$. Then Φ is tame at ∞.*

Proof. The hypothesis that all ∞-slopes of $\mathcal{F}$ are $\leq \sigma$ is that for all $y > \sigma$, the upper numbering subgroup $I(\infty)^y$ acts trivially on $\mathcal{F}$, i.e. dies in G_{geom}, and hence dies under Φ. Thus all ∞-slopes of $\mathcal{F}$ are $\leq \sigma$, and hence $\mathsf{Swan}_\infty(\Phi) \leq d\sigma < 1$. As Swan conductors are non-negative integers, $\mathsf{Swan}_\infty(\Phi) = 0$. This means $P(\infty)$ acts trivially in Φ, i.e. Φ is tame at ∞. □

Now we prove a generalization of [KT1, Theorem 4.16]:

Theorem 2.5. *Let U be a dense open set of $\mathbb{A}^1/\overline{\mathbb{F}_p}$, $\mathcal{F}$ a lisse $\overline{\mathbb{Q}_\ell}$-sheaf on U, with $\ell \neq p$, and let G be the geometric monodromy group of $\mathcal{H}$. Suppose that the following hold:*

(a) *All ∞-slopes of $\mathcal{H}$ are at most σ for some $0 < \sigma < 1$, and $\mathcal{H}$ is not tame at ∞;*

(b) *G is a finite almost quasisimple group: $S \lhd G/\mathbf{Z}(G) \leq \mathrm{Aut}(S)$ for some finite non-abelian simple group S;*

(c) *For some normal subgroup R of $G/\mathbf{Z}(G)$ containing S, R admits either a faithful d-dimensional linear representation*

$$\Phi : R \to \mathrm{GL}_d(\mathbb{F}),$$

or an e-dimensional projective representation

$$\Psi : R \to \mathrm{PGL}_e(\mathbb{F})$$

which is nontrivial over S, over some algebraically closed field $\mathbb{F}$ of characteristic $\neq p$.
Then

$$1/\sigma \leq d \cdot [G/\mathbf{Z}(G) : R] \leq d \cdot |\mathrm{Out}(S)|,$$

respectively

$$1/\sigma \leq (e^2-1) \cdot [G/\mathbf{Z}(G) : R] \leq (e^2-1) \cdot |\mathrm{Out}(S)|.$$

Proof. Note that the given Ψ is faithful. Indeed, $\mathrm{Ker}(\Psi) \lhd R$ does not contain S, so it intersects S trivially by simplicity of S. Because both S and $\mathrm{Ker}(\Psi)$ are normal in R, the commutator $[S, \mathrm{Ker}(\Psi)] \subset S \cap \mathrm{Ker}(\Psi) = 1$. Thus $\mathrm{Ker}(\Psi) \leq \mathbf{C}_R(S) \leq \mathbf{C}_{\mathrm{Aut}(S)}(S) = 1$. Hence R is embedded in $\mathrm{PGL}(U)$, where $U = \mathbb{F}^e$. Composing this embedding with the faithful action of $\mathrm{PGL}(U)$ on $\mathrm{End}^0(U) = \mathrm{End}(U)/\text{scalars}$, we obtain a faithful action of R on a module of dimension $\leq e^2 - 1$. Thus it suffices to prove the bound $1/\sigma \leq d \cdot [G/\mathbf{Z}(G) : R]$ when $\Phi : R \to \mathrm{GL}(V)$ is given.

So assume the contrary: $\Phi : R \to \mathrm{GL}(V)$ is faithful for some V with $\dim(V) = d$, but

$$1/\sigma > d \cdot [G/\mathbf{Z}(G) : R]. \tag{2.5.1}$$

Let $\tilde{V}$ denote the $\bar{G}$-module $\mathrm{Ind}_R^{\bar{G}}(V)$ for $\bar{G} := G/\mathbf{Z}(G)$. Note that $\bar{G}$ acts faithfully on $\tilde{V}$. Indeed, let $K \lhd \bar{G}$ denote the kernel of the action of $\bar{G}$ on $\tilde{V}$. By the construction of V as the induced representation, the R-module $\tilde{V}$ contains V as a submodule. But S acts faithfully on V, hence $S \cap K = 1$. As $S \lhd \bar{G}$, it follows that $[S, K] = 1$, and so

$$K \leq \mathbf{C}_{\bar{G}}(S) \leq \mathbf{C}_{\mathrm{Aut}(S)}(S) = 1.$$

We also note that

$$\dim(\tilde{V}) = [\bar{G} : R] \cdot \dim(V) = d \cdot [\bar{G} : R] < 1/\sigma$$

by (2.5.1).

Now view $\tilde{V}$ as a representation of G, of dimension $< 1/\sigma$. By Theorem 2.4, this representation is tame at ∞. Thus the image Q in G of $P(\infty)$ acts trivially on $\tilde{V}$. But $G/\mathbf{Z}(G)$ acts faithfully on $\tilde{V}$. Therefore Q lands in $\mathbf{Z}(G)$. Recall that $I(\infty)$ has finite image J in G, and J/Q is cyclic. As $Q \leq \mathbf{Z}(J)$, it follows that J is abelian. Thus all simple J-summands in $\mathcal{H}$ are one-dimensional, and at least one of them is wild, as $\mathcal{H}$ is not tame at ∞. Each one-dimensional wild component has Swan a strictly positive integer, which is also its slope, contradicting the hypothesis that all ∞-slopes of $\mathcal{H}$ are < 1. □

3. Primitive prime divisors for Suzuki-Ree groups

The order of a finite group of Lie type $G(\mathbb{F}_q)$ over a field $\mathbb{F}_q$ is usually a product of a power of $q = p^f$ (p the defining characteristic) and the values at q of cyclotomic polynomial $\Phi_m(q)$ for various m. In a number of problems on $G(\mathbb{F}_q)$, the existence of primitive prime divisors $\mathrm{ppd}(q, m)$ or $\mathrm{ppd}(p, mf)$ for certain m was helpful. Recall [Zs] that for $a, m \in \mathbb{Z}_{\geq 2}$, a *primitive prime divisor* $\ell = \mathrm{ppd}(a, m)$ is a prime divisor of $a^m - 1$ that does not divide $\prod_{i=1}^{m-1}(a^i - 1)$; such a prime divisor always exists unless $(a, m) = (2, 6)$ or $m = 2$ and $a + 1$ is a 2-power. For the Suzuki-Ree groups ${}^2B_2(q)$ with $q = 2^n$, $2 \nmid n \geq 3$, ${}^2G_2(q)$ with $q = 3^n$, $2 \nmid n \geq 3$, and ${}^2F_4(q)$ with $q = 2^n$, $2 \nmid n \geq 3$, some factor $\Phi_m(q)$ of $|G(\mathbb{F}_q)|$ decomposes further into values at $\sqrt{q}$ of polynomials over $\mathbb{Z}[\sqrt{2}]$ or $\mathbb{Z}[\sqrt{3}]$. More precisely,

$$\Phi_4(q) = q^2 + 1 = (q - \sqrt{2q} + 1)(q + \sqrt{2q} + 1)$$

for ${}^2B_2(q)$,

$$\Phi_6(q) = q^2 - q + 1 = (q - \sqrt{3q} + 1)(q + \sqrt{3q} + 1)$$

for ${}^2G_2(q)$, and

$$\Phi_{12}(q) = q^4 - q^2 + 1 = (q^2 - q\sqrt{2q} + q - \sqrt{2q} + 1)(q^2 + q\sqrt{2q} + q + \sqrt{2q} + 1)$$

for ${}^2F_4(q)$. In applications, it is desirable to prove that these factors also possess primitive prime divisors $\mathrm{ppd}(p, 4n)$, respectively $\mathrm{ppd}(p, 6n)$, $\mathrm{ppd}(p, 12n)$, whose existence does not follow from [Zs]. The main results of this section establish the existence of such prime divisors for Suzuki-Ree groups.

3A. Almost equidistribution of coprime integers in congruence classes. For $n \in \mathbb{Z}_{\geq 1}$, let $\phi(n)$ denote the Euler function of n, let $\mu(n)$ denote the Möbius function of n, and let $\omega(n)$ denote the number of distinct prime divisors of n (not counting multiplicities). First we prove the following

Proposition 3.1. *Let $m, n \in \mathbb{Z}_{\geq 1}$ be coprime integers. For any integer $0 \leq a \leq m-1$, the number N_a of integers $1 \leq k \leq n$ such that $\gcd(k, n) = 1$ and $k \equiv a \pmod m$ satisfies*

$$\big|N_a - \frac{\phi(n)}{m}\big| < 2^{\omega(n)}.$$

Proof. For $k \in \mathbb{Z}_{\geq 1}$, define $F(k) := 0$ if $\gcd(k, n) > 1$ and $F(k) := 1$ if $\gcd(k, n) = 1$. By [MNZ, Theorem 4.7], $F(k) = \sum_{d \mid \gcd(k,n)} \mu(d)$. Now

$$N_a = \sum_{1 \leq k \leq n,\ k \equiv a \pmod m} F(k) = \sum_{1 \leq k \leq n,\ k \equiv a \pmod m} \sum_{d \mid \gcd(k,n)} \mu(d) = \sum_{d \mid n} \mu(d) N(a, d), \tag{3.1.1}$$

with

$$N(a, d) := \sum_{1 \leq k \leq n,\ k \equiv a \pmod m,\ d \mid k} 1.$$

If $d|n$, then $\gcd(d, m) = 1$, so we can find $1 \leq e \leq m-1$ such that $de \equiv 1 \pmod m$. Now write every $1 \leq k \leq n$ with $d|k$ as $k = dl$ with $1 \leq l \leq n/d$. Then the condition that $k \equiv a \pmod m$ is equivalent to $l \equiv ea \pmod m$, in which case we can write $l = s + mi$ with $0 \leq r \leq m-1$, $ea \equiv r \pmod m$, and $i \in \mathbb{Z}$. To count the number $N(a, d)$ of i occurring, write $n/d = qm + r$ with $0 \leq r \leq m-1$ and $q \in \mathbb{Z}_{\geq 0}$. Certainly, every $0 \leq i \leq q-1$ works, but neither $i = -1$ nor $i = q+1$ can occur. It follows that

$$n/md - 1 < q \leq N(a, d) \leq q + 1 < n/md + 1. \tag{3.1.2}$$

We also note by [MNZ, (4.1)] that $\phi(n) = \sum_{d|n} \mu(d) n/d$ and that $\sum_{d|n} |\mu(d)|$ is the number of square-free divisors of n and hence equals to $2^{\omega(n)}$. Combining with (3.1.1) and (3.1.2), this yields

$$\big|N_a - \frac{\phi(n)}{m}\big| = \big|\sum_{d|n} \mu(d)(N(a, d) - n/md)\big| < \sum_{d|n} |\mu(d)| = 2^{\omega(n)}.$$

□

We will also need the following analogue of Proposition 3.1:

Proposition 3.2. *Let $n \in \mathbb{Z}_{\geq 1}$ be an odd integer divisible by 3. For any integer $0 \leq a \leq 11$ coprime to 3, the number N_a of integers $1 \leq k \leq n$ such that $\gcd(k, n) = 1$ and $k \equiv a \pmod{12}$ satisfies*

$$\big|N_a - \frac{\phi(n)}{8}\big| < 2^{\omega(n)-1}.$$

Proof. As in the proof of Proposition 3.2, we have

$$N_a = \sum_{1 \leq k \leq n,\ k \equiv a \pmod{12}} F(k) = \sum_{1 \leq k \leq n,\ k \equiv a \pmod{12}} \sum_{d \mid \gcd(k,n)} \mu(d) = \sum_{d \mid n} \mu(d) N(a, d),$$

with

$$N(a,d) := \sum_{1\le k\le n,\ k\equiv a \,(\mathrm{mod}\ 12),\ d|k} 1.$$

Now, if $d|n$ but $3|d$, then $N(a,d)=0$ since $3\nmid a$. Hence,

$$N_a = \sum_{d|n,\ 3\nmid d} \mu(d)N(a,d). \tag{3.2.1}$$

Next, $\mu(d)=0$ if $9|d$, and $\mu(d)=-\mu(d/3)$ if $3|d$. It follows from [MNZ, (4.1)] that

$$\frac{\phi(n)}{n} = \sum_{d|n}\frac{\mu(d)}{d} = \sum_{d|n,\ 3\nmid d}\frac{\mu(d)}{d} - \sum_{3d'=d|n, 3\nmid d'}\frac{\mu(d')}{3d'} = \frac{2}{3}\sum_{d|n,\ 3\nmid d}\frac{\mu(d)}{d}. \tag{3.2.2}$$

If $d|n$ and $3\nmid d$, then $\gcd(d,12)=1$, so we can find $1\le e\le 11$ such that $de\equiv 1 \,(\mathrm{mod}\ 12)$. The proof of (3.1.2) repeated verbatim shows that

$$n/12d - 1 < q \le N(a,d) \le q+1 < n/12d+1.$$

Combining with (3.2.1) and (3.2.2), this yields

$$\big|N_a - \frac{\phi(n)}{8}\big| = \big|\sum_{d|n,\ 3\nmid d}\mu(d)(N(a,d)-n/12d)\big| < \sum_{d|n,\ 3\nmid d}|\mu(d)| = 2^{\omega(n)-1}.$$

□

3B. Primitive prime divisor for Suzuki groups. We make the choice $\sqrt{2}>0$. For odd $n\in\mathbb{Z}_{\ge 1}$ and $a=1,3$, set

$$P_{2,a}(n) := \prod_{1\le k<8n,\ \gcd(k,n)=1,\ k\equiv a \,(\mathrm{mod}\ 8)} \big(3-2\sqrt{2}\cos\frac{k\pi}{4n}\big).$$

Proposition 3.3. *If $2\nmid n\ge 2603$ and $a=1,3$, then $P_{2,a}(n)>2n$.*

Proof. (i) First we note that

$$\phi(n) \ge \max\big(2^{2.2\omega(n)}, n^{6/7}\big) \tag{3.3.1}$$

when $2\nmid n$ and $n\ne 1,3,9,15,21,33,45,75,105,165,195$. Indeed, suppose $s:=\omega(n)\ge 1$ and write $n=\prod_{i=1}^s p_i^{a_i}$ for some prime divisors $2<p_1<p_2<\ldots<p_s$ of n. If $p_1\ge 5$, then

$$\frac{n}{\phi(n)} = \prod_{i=1}^s \frac{p_i}{p_i-1} \le (5/4)^s < 5^{s/7} \le n^{1/7},$$

and so $\phi(n)>n^{6/7}$. If $p_1\ge 7$, then

$$\phi(n) = \prod_{i=1}^s p_i^{a_i}(1-1/p_i) \ge 6^s > 2^{2.5s}.$$

If $p_1=5$ and $s\ge 2$, then

$$\phi(n) = \prod_{i=1}^s p_i^{a_i}(1-1/p_i) \ge 4\cdot 6^{s-1} > 2^{2.25s}.$$

If $p_1=5$ and $s=1$, but $n\ne 5$ then $\phi(n)\ge 20>2^{4s}$.

In the rest of the proof of (3.3.1), we may assume that $p_1 = 3$. First suppose that $s \geq 4$. As $(11^6/10^7)^{s-3} < (2\cdot 4\cdot 6)^7/(3\cdot 5\cdot 7)^6$,

$$\frac{n}{\phi(n)} = \prod_{i=1}^{s} \frac{p_i}{p_i - 1} \leq \frac{3}{2}\cdot\frac{5}{4}\cdot\frac{7}{6}\cdot\left(\frac{11}{10}\right)^{s-3} < \left(3\cdot 5\cdot 7\cdot 11^{s-3}\right)^{1/7} < n^{1/7}.$$

Also, $\phi(n) \geq 2\cdot 4\cdot 6\cdot 10^{s-3} > 2^{2.23s}$.

Next suppose that $s = 3$. If $p_3 \geq 11$, then

$$\frac{n}{\phi(n)} = \prod_{i=1}^{s} \frac{p_i}{p_i - 1} \leq \frac{3}{2}\cdot\frac{5}{4}\cdot\frac{11}{10} < \left(3\cdot 5\cdot 11\right)^{1/7} < n^{1/7}.$$

If $p_3 < 11$ then $(p_1, p_2, p_3) = (3, 5, 7)$; thus if $n \neq 105$ then $n > 3\cdot 105$ and so

$$n/\phi(n) = (3\cdot 5\cdot 7)/(2\cdot 4\cdot 6) < n^{1/7}.$$

Also, if $n \neq 105, 165, 195$, then $\phi(n) \geq 2\cdot 6\cdot 10 > 2^{2.2s}$.

Suppose now that $s = 2$. If $p_2 \geq 13$, then $n/\phi(n) \leq (3/2)\cdot(13/12) < (3\cdot 13)^{1/7} \leq n^{1/7}$. If $p_3 = 11$ and $n \neq 33$, then $n/\phi(n) = (3/2)\cdot(11/10) < (3\cdot 3\cdot 11)^{1/7} \leq n^{1/7}$. If $p_3 = 7$ and $n \neq 21$, then $n/\phi(n) = (3/2)\cdot(7/6) < (3\cdot 3\cdot 7)^{1/7} \leq n^{1/7}$. If $p_3 = 5$ and $n \neq 15, 45, 75$, then $n/\phi(n) = (3/2)\cdot(5/4) < (6\cdot 3\cdot 5)^{1/7} < n^{1/7}$. Also, if $n \neq 15, 21, 33, 45$, then $\phi(n) \geq 24 > 2^{2.2s}$.

Finally, assume that $s = 1$, and $n = 3^a$ with $a \geq 3$. Then $n/\phi(n) = 3/2 < 3^{a/7} = n^{1/7}$, and $\phi(n) \geq 18 > 2^{4s}$, completing the proof of (3.3.1).

(ii) Now assume that $n \geq 2602$. By (3.3.1) $m := \phi(n) \geq n^{6/7} > 846$, so $m \geq 847$, and $2^{\omega(n)} \leq m^{5/11}$.

Fix $a \in \{1, 3\}$ and let $S_j := \{(j-1)n \leq k < jn \mid \gcd(k, 8n) = 1, k \equiv a \pmod 8\}$ for $0 \leq j \leq 7$. For each j, observe that $k \in S_j$ if and only if $0 \leq k' := k - jn < n$ is coprime to n and $k' \equiv a - jn \pmod 8$. By Proposition 3.1,

$$|S_j| = |\{0 \leq k' < n \mid \gcd(k, n) = 1, k' \equiv a - jn \pmod 8\}|$$

satisfies $\phi(n)/8 - 2^{\omega(n)} < |S_j| < \phi(n)/8 + 2^{\omega(n)}$. By the above,

$$m/8 - m^{5/11} < |S_j| < m/8 + m^{5/11}. \tag{3.3.2}$$

Now, if $k \in S_0 \cup S_7$, then $3 - 2\sqrt{2}\cos(k\pi/4n) \geq 3 - 2\sqrt{2}$. If $k \in S_1 \cup S_6$, then $3 - 2\sqrt{2}\cos(k\pi/4n) \geq 1$. If $k \in S_2 \cup S_5$, then $3 - 2\sqrt{2}\cos(k\pi/4n) \geq 3$. Finally, if $k \in S_3 \cup S_4$, then $3 - 2\sqrt{2}\cos(k\pi/4n) \geq 5$. It follows from (3.3.2) that

$$P_{2,a}(n) \geq (3 - 2\sqrt{2})^{m/4 + 2m^{5/11}} \cdot 15^{m/4 - 2m^{5/11}} = A^{m/4} B^{-2m^{5/11}}$$

with $A := 15(3 - 2\sqrt{2})$ and $B := 15(3 + 2\sqrt{2})$.

Setting $f(t) := A^{t/4} B^{-2t^{5/11}} t^{-7/6}$,

$$g(t) := \log f(t) = (t/4)\log(A) - 2t^{5/11}\log(B) - (7/6)\log(t).$$

Now $g'(t) = \log(A)/4 - \log(B)/(1.1t^{6/11}) - (7/6t)$ is increasing, so $g'(t) \geq g'(847) > 0.13$ when $t \geq 847$. It follows that $g(m) \geq g(847) > 0.75$, and so $f(m) = \exp(g(m)) > 2.11$. Thus, for $m = \phi(n) \geq 847$

$$P_{2,a}(n) \geq f(m) m^{7/6} > 2m^{7/6} > 2n,$$

as desired. □

As we will see in part (iii) of the proof of the following theorem, Proposition 3.3 actually holds for all odd $n \geq 7$.

Theorem 3.4. *Let $q = 2^n$ with $2 \nmid n$. If $n \geq 7$ then $t(q) = t^-(q) := q - \sqrt{2q} + 1$ is divisible by a primitive prime divisor* $\mathrm{ppd}(2, 4n)$ *of $q^2 + 1$. In all cases, $t^+(q) := q + \sqrt{2q} + 1$ is divisible by a primitive prime divisor* $\mathrm{ppd}(2, 4n)$ *of $q^2 + 1$.*

Proof. (i) The second statement is obvious for $n \leq 5$; also note that $t(2) = 1$, $t(8) = 5$. Henceforth we may assume $n \geq 7$. Consider the sets

$$A_j := \{1 \leq k \leq 4n \mid \gcd(k, 2n) = 1,\ k \equiv j \pmod 8\},$$
$$B_j := \{4n + 1 \leq k \leq 8n \mid \gcd(k, 2n) = 1, k \equiv j \pmod 8\}$$

for $j = 1, 3, 5, 7$. Then the map $k \mapsto 8n - k$ yields bijections

$$A_1 \longleftrightarrow B_7,\ A_7 \longleftrightarrow B_1,\ A_3 \longleftrightarrow B_5,\ A_5 \longleftrightarrow B_3,$$

and the map $k \mapsto k + 4n$ yields bijections

$$A_1 \longleftrightarrow B_5,\ A_5 \longleftrightarrow B_1,\ A_3 \longleftrightarrow B_7,\ A_7 \longleftrightarrow B_3.$$

It follows that

$$|A_1| = |A_3| = |B_5| = |B_7|,\ |A_5| = |A_7| = |B_1| = |B_3|. \tag{3.4.1}$$

Since $\sqcup_{j=1,3,5,7}\big(A_j \sqcup B_j\big) = \{1 \leq k < 8n \mid \gcd(k, 8n) = 1\}$, we now see that

$$|A_j| + |B_j| = \phi(8n)/4 = \phi(n) \tag{3.4.2}$$

for each $j = 1, 3, 5, 7$.

(ii) Make the choice of $\zeta := \zeta_{8n} = \exp(\pi i/4n)$ and consider the cyclotomic polynomial

$$\Phi_{8n}(X) = \prod_{1 \leq k < 8n,\ \gcd(k,2n)=1} \big(X - \zeta^k\big).$$

If $1 \leq k < 4n$ then $(X - \zeta^k)(X - \zeta^{k+4n}) = (X - \zeta^k)(X + \zeta^k) = X^2 - \zeta_{4n}^k$. It follows that

$$\Phi_{8n}(X) = \prod_{1 \leq k < 4n,\ \gcd(k,2n)=1} \big(X^2 - \zeta_{4n}^k\big) = \Phi_{4n}(X^2).$$

In particular,

$$\Phi_{4n}(2) = \Phi_{8n}(\sqrt{2}). \tag{3.4.3}$$

Setting

$$\Phi_{8n,a}(X) := \prod_{1 \leq k < 8n,\ \gcd(k,2n)=1,\ k \equiv \pm a \pmod 8} \big(X - \zeta^k\big), \tag{3.4.4}$$

for $a = 1, 3$, we have $\Phi_{8n}(X) = \Phi_{8n,1}(X)\Phi_{8n,3}(X)$. Next, since

$$(\sqrt{2} - \zeta^k)(\sqrt{2} - \zeta^{8n-k}) = 3 - 2\sqrt{2}\cos\frac{k\pi}{4n}$$

for each $1 \leq k < 8n$, using the bijection $k \mapsto 8n - k$ in (3.4.1)

$$P_{2,a}(n) = \Phi_{8n,a}(\sqrt{2}), \tag{3.4.5}$$

for $a = 1, 3$. Using (3.4.3) also

$$P_{2,1}(n)P_{2,3}(n) = \Phi_{4n}(2). \tag{3.4.6}$$

(iii) To show that $P_{2,1}(n)$ and $P_{2,3}(n)$ are integers, we use $\gcd(8, n) = 1$ to write $1 = ns + 8t$ for some $s, t \in \mathbb{Z}$ with $\gcd(s, 8) = \gcd(t, n) = 1$, and set $\zeta = \zeta_{8n} = \alpha\beta$ with $\alpha := \zeta^{ns}$, a 8^{th} root of unity, and $\beta := \zeta^{8t}$, an n^{th} root of unity. When k runs over $A_1 \sqcup B_1$, $\zeta^k = \alpha^k\beta^k = \alpha\beta^k$, and

$k \pmod n$ runs over units in $\mathbb{Z}/n\mathbb{Z}$, each at most once. Using (3.4.2), we see that each unit is met exactly once. Repeating the same argument for $k \in A_7 \sqcup B_7$, we get

$$\Phi_{8n,1}(X) := \prod_{l \text{ unit mod } n} \big(X - \alpha\beta^l\big)\big(X - \alpha^{-1}\beta^l\big) = \prod_{l \text{ unit mod } n} (X^2 - (\alpha + \alpha^{-1})\zeta_n^l X + \zeta_n^{2l}).$$

Note that $\alpha + \alpha^{-1} = \epsilon\sqrt{2}$ for some $\epsilon = \pm 1$. It follows from (3.4.5) that

$$P_{2,1}(n) = \Phi_{8n,1}(\sqrt{2}) = \prod_{l \text{ unit mod } n} (2 - 2\epsilon\zeta_n^l + \zeta_n^{2l})$$

is the norm $\mathrm{Norm}_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}$ of the algebraic integer $2 - 2\epsilon\zeta_n + \zeta_n^2$, hence it is an integer. The same arguments show that $P_{2,3}(n)$ is the norm $\mathrm{Norm}_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}$ of the algebraic integer $2 + 2\epsilon\zeta_n + \zeta_n^2$, hence it is an integer.

Using this norm interpretation for $P_{2,1}(n)$ and $P_{2,3}(n)$, a calculation with Magma shows that $P_{2,a}(n) > 2n$ for odd integers $7 \le n \le 2601$. Together with Proposition 3.3, this shows that

$$P_{2,a}(n) > 2n \tag{3.4.7}$$

for $a = 1, 3$ and odd $n \ge 7$.

(iv) We also set

$$f^-(X) := X^{2n} - \sqrt{2}X^n + 1,\ f^+(X) := X^{2n} + \sqrt{2}X^n + 1,$$

so that

$$t^-(q) = f^-(\sqrt{(}2)),\ t^+(q) = f^+(\sqrt{(}2)),\ f^-(X)f^+(X) = X^{4n} + 1.$$

Certainly, any root of $X^{4n} + 1$ is ζ^k for some odd integer $1 \le k < 8n$. If $k \equiv \pm 1 \pmod 8$, then

$$f^-(\zeta^k) = \exp(k\pi i/2) + 1 - \sqrt{2}\exp(k\pi i/4) = 0.$$

Similarly, if $k \equiv \pm 3 \pmod 8$, then

$$f^+(\zeta^k) = \exp(k\pi i/2) + 1 + \sqrt{2}\exp(k\pi i/4) = 0.$$

It follows that

$$f^-(X) = \prod_{1 \le k < 8n,\ k \equiv \pm 1 \,(\mathrm{mod}\ 8)} \big(X - \zeta^k\big),\ f^+(X) = \prod_{1 \le k < 8n,\ k \equiv \pm 3 \,(\mathrm{mod}\ 8)} \big(X - \zeta^k\big).$$

Comparing to (3.4.4) and (3.4.5), we see that

$$f^-(\sqrt{2})/P_{2,1}(n) = \prod_{1 \le k < 8n,\ \gcd(k,2n) > 1,\ k \equiv \pm 1 \,(\mathrm{mod}\ 8)} \big(\sqrt{2} - \zeta^k\big)$$

is an algebraic integer. But $f^-(\sqrt{2}) = t^-(q)$ is an integer, and $P_{2,1}(n)$ is an integer by (iii). Hence $P_{2,1}(n)$ divides $t^-(q)$. Similarly, $P_{2,3}(n)$ divides $t^+(q)$.

(v) By (3.4.7), $P_{2,1}(n) > n$. Consider any prime divisor ℓ of $P_{2,1}(n)$, which then divides $t^-(q)$ by the result of (iv), and divides $\Phi_{4n}(2)$ by (3.4.6). Suppose that ℓ is not a primitive prime divisor of $2^{4n} - 1$. By [Lun, Satz 1] (cf. [Ro, Proposition 2]) $\ell | n$, and moreover $\ell^2 \nmid \Phi_{4n}(2)$. It follows that the ℓ-part of $P_{2,1}(n)$ is ℓ. Hence, if $t^-(q)$ is not divisible by any primitive prime divisor of $2^{4n} - 1$, then $P_{2,1}(n)$ divides n, a contradiction.

The proof for $t^+(q)$ is entirely similar. □

Corollary 3.5. *Let $q = 2^n$ with $2 \nmid n$. If $n \ge 3$ then $\Phi''_{24} := q^2 - q\sqrt{2q} + q - \sqrt{2q} + 1$ is divisible by a primitive prime divisor* $\mathrm{ppd}(2, 12n)$ *of $q^4 - q^2 + 1$. In all cases, $\Phi'_{24} := q^2 + q\sqrt{2q} + q + \sqrt{2q} + 1$ is divisible by a primitive prime divisor* $\mathrm{ppd}(2, 12n)$ *of $q^4 - q^2 + 1$.*

Proof. Note that if $n = 1$ then $\Phi''_{24} = 1$ and $\Phi'_{24} = 13$. Assume that $n \geq 3$. By Theorem 3.4,

$$t^-(q^3) = q^3 - q\sqrt{2q} + 1 = (q + \sqrt{2q} + 1)(q^2 - q\sqrt{2q} + q - \sqrt{2q} + 1) = t^+(q)\Phi''_{24}$$

is divisible by a primitive prime divisor $\ell_1 = \mathrm{ppd}(2, 12n)$. Since $t^+(q)|(q^2+1)$ and $\ell_1|(q^4 - q^2 + 1)$, we see that $\ell_1 \nmid t^+(q)$, and so $\ell_1|\Phi''_{24}$. The argument for Φ'_{24} is similar, using

$$t^+(q^3) = q^3 + q\sqrt{2q} + 1 = (q - \sqrt{2q} + 1)(q^2 + q\sqrt{2q} + q + \sqrt{2q} + 1) = t^-(q)\Phi'_{24}.$$

□

3C. Primitive prime divisor for Ree groups. The results in this subsection are not needed for the rest of the paper, however they will be used elsewhere [KT2]. We make the choice $\sqrt{3} > 0$. For odd $n \in \mathbb{Z}_{\geq 1}$ and $a = 1, 5$, set

$$P_{3,a}(n) := \prod_{1 \leq k < 12n,\ \gcd(k,n)=1,\ k \equiv a \,(\mathrm{mod}\ 12)} \big(4 - 2\sqrt{3}\cos\frac{k\pi}{6n}\big).$$

Proposition 3.6. *If $2 \nmid n \geq 3$ and $a = 1, 5$, then $P_{3,a}(n) > 2n$.*

Proof. A computation with Mathematica shows that $P_{3,a}(n) > 2n$ when $3 \leq n \leq 353$. Now assume that $n \geq 354$. By (3.3.1) $m := \phi(n) \geq n^{6/7} > 153$, so $m \geq 154$, and $2^{\omega(n)} \leq m^{5/11}$.

Fix $a \in \{1, 5\}$ and let $R_j := \{(j-1)n \leq k < jn \mid \gcd(k, 12n) = 1, k \equiv a \,(\mathrm{mod}\ 12)\}$ for $0 \leq j \leq 11$. For each j, observe that $k \in R_j$ if and only if $0 \leq k' := k - jn < n$ is coprime to n and $k' \equiv a - jn \,(\mathrm{mod}\ 12)$. If $3 \nmid n$, then according to Proposition 3.1,

$$|R_j| = |\{0 \leq k' < n \mid \gcd(k, n) = 1, k' \equiv a - jn \,(\mathrm{mod}\ 12)\}|$$

satisfies $\phi(n)/12 - 2^{\omega(n)} < |R_j| < \phi(n)/12 + 2^{\omega(n)}$. On the other hand, if $3|n$ then $3 \nmid (a - jn)$, so by Proposition 3.2,

$$|R_j| = |\{0 \leq k' < n \mid \gcd(k, n) = 1, k' \equiv a - jn \,(\mathrm{mod}\ 12)\}|$$

satisfies $\phi(n)/8 - 2^{\omega(n)-1} < |R_j| < \phi(n)/8 + 2^{\omega(n)-1}$.

Setting $b := 12$ when $3 \nmid n$ and $b := 8$ when $3|n$, by the above consideration now

$$m/b - m^{5/11} < |R_j| < m/b + m^{5/11}. \tag{3.6.1}$$

Now, if $k \in S_0 \cup S_{11}$, then $4 - 2\sqrt{3}\cos(k\pi/6n) \geq 4 - 2\sqrt{3}$. If $k \in S_1 \cup S_{10}$, then $4 - 2\sqrt{3}\cos(k\pi/6n) \geq 1$. If $k \in S_2 \cup S_9$, then $4 - 2\sqrt{3}\cos(k\pi/6n) \geq 4 - \sqrt{3}$. If $k \in S_3 \cup S_8$, then $4 - 2\sqrt{3}\cos(k\pi/6n) \geq 4$. If $k \in S_4 \cup S_7$, then $4 - 2\sqrt{3}\cos(k\pi/6n) \geq 4 + \sqrt{3}$. Finally, if $k \in S_5 \cup S_6$, then $4 - 2\sqrt{3}\cos(k\pi/6n) \geq 7$. It follows from (3.6.1) that

$$\begin{aligned} P_{3,a}(n) &\geq \big(4 - 2\sqrt{3}\big)^{2m/b + 2m^{5/11}} \cdot \big((4 - \sqrt{3}) \cdot 4 \cdot (4 + \sqrt{3}) \cdot 7\big)^{2m/b - 2m^{5/11}} \\ &= A^{2m/b} B^{-2m^{5/11}} \geq A^{m/6} B^{-2m^{5/11}} \end{aligned}$$

with $A := 364(4 - 2\sqrt{3})$ and $B := 364/(4 - 2\sqrt{3})$.

Setting $f(t) := A^{t/6} B^{-2t^{5/11}} t^{-7/6}$,

$$g(t) := \log f(t) = (t/6)\log(A) - 2t^{5/11}\log(B) - (7/6)\log(t).$$

Now $g'(t) = \log(A)/6 - \log(B)/(1.1t^{6/11}) - 7/6t$ is increasing, so $g'(t) \geq g'(154) > 0.48$ when $t \geq 154$. It follows that $g(m) \geq g(154) > 0.74$, and so $f(m) = \exp(g(m)) > 2.09$. Thus, for $m = \phi(n) \geq 154$

$$P_{3,a}(n) \geq f(m)m^{7/6} > 2m^{7/6} > 2n,$$

as desired. □

Theorem 3.7. *Let $q = 3^n$ with $2 \nmid n$. If $n \geq 3$ then $t(q) = t^-(q) := q - \sqrt{3q} + 1$ is divisible by a primitive prime divisor* $\mathrm{ppd}(3, 6n)$ *of $q^2 - q + 1$. In all cases, $t^+(q) := q + \sqrt{3q} + 1$ is divisible by a primitive prime divisor* $\mathrm{ppd}(3, 6n)$ *of $q^2 - q + 1$.*

Proof. (i) Note that $t(3) = 1$. Henceforth we will assume $n \geq 3$. Consider the sets

$$A_j := \{1 \leq k \leq 6n \mid \gcd(k, 12n) = 1,\ k \equiv j \pmod{12}\},$$
$$B_j := \{6n + 1 \leq k \leq 12n \mid \gcd(k, 12n) = 1, k \equiv j \pmod{12}\}$$

for $j = 1, 5, 7, 11$. Then the map $k \mapsto 12n - k$ yields bijections

$$A_1 \longleftrightarrow B_{11},\ A_{11} \longleftrightarrow B_1,\ A_5 \longleftrightarrow B_7,\ A_7 \longleftrightarrow B_5,$$

and the map $k \mapsto k + 6n$ yields bijections

$$A_1 \longleftrightarrow B_7,\ A_7 \longleftrightarrow B_1,\ A_5 \longleftrightarrow B_{11},\ A_{11} \longleftrightarrow B_5.$$

It follows that

$$|A_1| = |A_5| = |B_7| = |B_{11}|,\ |A_7| = |A_{11}| = |B_1| = |B_5|. \tag{3.7.1}$$

Since $\sqcup_{j=1,5,7,11}\big(A_j \sqcup B_j\big) = \{1 \leq k < 12n \mid \gcd(k, 12n) = 1\}$, we now see that

$$|A_j| + |B_j| = \phi(12n)/4 = \phi(3n)/2 \tag{3.7.2}$$

for each $j = 1, 5, 7, 11$.

(ii) Make the choice of $\zeta := \zeta_{12n} = \exp(\pi i/6n)$ and consider the cyclotomic polynomial

$$\Phi_{12n}(X) = \prod_{1 \leq k < 12n,\ \gcd(k,12n)=1} \big(X - \zeta^k\big).$$

If $1 \leq k < 6n$ then $(X - \zeta^k)(X - \zeta^{k+6n}) = (X - \zeta^k)(X + \zeta^k) = X^2 - \zeta_{6n}^k$. It follows that

$$\Phi_{12n}(X) = \prod_{1 \leq k < 6n,\ \gcd(k,6n)=1} \big(X^2 - \zeta_{6n}^k\big) = \Phi_{6n}(X^2).$$

In particular,

$$\Phi_{6n}(3) = \Phi_{12n}(\sqrt{3}). \tag{3.7.3}$$

Setting

$$\Phi_{12n,a}(X) := \prod_{1 \leq k < 12n,\ \gcd(k,12n)=1,\ k \equiv \pm a \pmod{12}} \big(X - \zeta^k\big), \tag{3.7.4}$$

for $a = 1, 5$, we have $\Phi_{12n}(X) = \Phi_{12n,1}(X)\Phi_{12n,5}(X)$. Next, since

$$(\sqrt{3} - \zeta^k)(\sqrt{3} - \zeta^{12n-k}) = 4 - 2\sqrt{3}\cos\frac{k\pi}{6n}$$

for each $1 \leq k < 12n$, using the bijection $k \mapsto 12n - k$ in (3.7.1)

$$P_{3,a}(n) = \Phi_{12n,a}(\sqrt{3}), \tag{3.7.5}$$

for $a = 1, 5$. Using (3.7.3) also

$$P_{3,1}(n)P_{3,5}(n) = \Phi_{6n}(3). \tag{3.7.6}$$

(iii) Here we show that $P_{3,1}(n)$ and $P_{3,5}(n)$ are integers. Clearly, they are algebraic integers in $\mathbb{Q}(\zeta)$. Hence it suffices to show that each of them is fixed by any Galois automorphism $\sigma : \zeta \mapsto \zeta^l$,

$\gcd(l, 12n) = 1$. First consider the case $j \equiv \pm 1 \pmod{12}$. Then σ fixes $\sqrt{3} = \zeta_{12} + \zeta_{12}^{-1}$, and fixes each of the sets $C := \sqcup_{j=1,11}(A_j \cup B_j)$ and $D := \sqcup_{j=1,11}(A_j \cup B_j)$ modulo $12n$. Since

$$P_{3,1}(n) = \prod_{k \in C}(\sqrt{3} - \zeta^k),\ P_{3,5}(n) = \prod_{k \in D}(\sqrt{3} - \zeta^k),$$

it follows that σ fixes each of $P_{3,1}(n)$ and $P_{3,5}(n)$. Now assume that $j \equiv \pm 5 \pmod{12}$. Then σ sends $\sqrt{3}$ to $-\sqrt{3}$ and ζ^k to ζ^{kl}, and thus

$$\sigma\big(\sqrt{3} - \zeta^k\big) = -\sqrt{3} - \zeta^{kl} = -\big(\sqrt{3} - \zeta^{6n+kl}\big).$$

Note that modulo $12n$, when k runs over C, $6n + kl$ runs over C, covering each element of C exactly once. Also, $|C| = \phi(3n)$ by (3.7.2), and so $|C|$ is even. It follows that σ sends $P_{3,1}(n)$ to $(-1)^{|C|}P_{3,1}(n) = P_{3,1}(n)$, and similarly σ fixes $P_{3,5}(n)$.

(iv) We also set

$$f^-(X) := X^{2n} - \sqrt{3}X^n + 1,\ f^+(X) := X^{2n} + \sqrt{3}X^n + 1,$$

so that

$$t^-(q) = f^-(\sqrt(3)),\ t^+(q) = f^+(\sqrt(3)),\ f^-(X)f^+(X) = X^{4n} - X^{2n} + 1.$$

Certainly, any root of $X^{4n} - X^{2n} + 1$ is ζ^k for some integer $1 \le k < 12n$ coprime to 6. If $k \equiv \pm 1 \pmod{12}$, then

$$f^-(\zeta^k) = \exp(k\pi i/3) + 1 - \sqrt{3}\exp(k\pi i/6) = 0.$$

Similarly, if $k \equiv \pm 5 \pmod{12}$, then

$$f^+(\zeta^k) = \exp(k\pi i/3) + 1 + \sqrt{3}\exp(k\pi i/6) = 0.$$

It follows that

$$f^-(X) = \prod_{1 \le k < 12n,\ k \equiv \pm 1 \pmod{12}} \big(X - \zeta^k\big),\ f^+(X) = \prod_{1 \le k < 12n,\ k \equiv \pm 5 \pmod{12}} \big(X - \zeta^k\big).$$

Comparing to (3.7.4) and (3.7.5), we see that

$$f^-(\sqrt{3})/P_{3,1}(n) = \prod_{1 \le k < 8n,\ \gcd(k,12n) > 1,\ k \equiv \pm 1 \pmod{12}} \big(\sqrt{3} - \zeta^k\big)$$

is an algebraic integer. But $f^-(\sqrt{3}) = t^-(q)$ is an integer, and $P_{3,1}(n)$ is an integer by (iii). Hence $P_{3,1}(n)$ divides $t^-(q)$. Similarly, $P_{3,5}(n)$ divides $t^+(q)$.

(v) By Proposition 3.6, $P_{3,1}(n) > n$. Consider any prime divisor ℓ of $P_{3,1}(n)$, which then divides $t^-(q)$ by the result of (iv), and divides $\Phi_{6n}(3)$ by (3.7.6). Since $\ell | (q^2 - q + 1)$, $\ell \ne 2, 3$. Suppose that ℓ is not a primitive prime divisor of $3^{6n} - 1$. Again by [Lun, Satz 1] $\ell | 3n$, whence $\ell | n$ as $\ell \ge 5$, and moreover $\ell^2 \nmid \Phi_{6n}(3)$. It follows that the ℓ-part of $P_{3,1}(n)$ is ℓ. Hence, if $t^-(q)$ is not divisible by any primitive prime divisor of $3^{6n} - 1$, then $P_{3,1}(n)$ divides n, a contradiction.

The proof for $t^+(q)$ is entirely similar. □

3D. Primitive prime divisors for Suzuki-Ree groups: another approach. For $\delta \in \mathbb{Z}^+$, $\alpha \in (\mathbb{Z}/\delta)^\times$, and $x \in \mathbb{R}^+$ with $x \ge 1$, let

$$f_n^{(\alpha \bmod \delta)}(x) := \prod_{a \in (\mathbb{Z}/\delta n)^\times : a \equiv \pm\alpha \pmod{\delta}} (x - \zeta_{\delta n}^a).$$

Note that for such δ, α, and x, $f_n^{(\alpha \bmod \delta)}(x) \in \mathbb{R}^+$ by pairing a with $-a$. Note also that

$$\begin{aligned} f_n^{(1 \bmod 8)}(\sqrt{2}) &= P_{2,1}(n) = \Phi_{8n,1}(\sqrt{2}), \\ f_n^{(3 \bmod 8)}(\sqrt{2}) &= P_{2,3}(n) = \Phi_{8n,3}(\sqrt{2}), \\ f_n^{(1 \bmod 12)}(\sqrt{3}) &= P_{3,1}(n) = \Phi_{12n,1}(\sqrt{3}), \\ f_n^{(5 \bmod 12)}(\sqrt{3}) &= P_{3,5}(n) = \Phi_{12n,5}(\sqrt{3}) \end{aligned}$$

in the notation above.

Lemma 3.8. *Let $n \in \mathbb{Z}^+$. Let $x \geq 1$. Then*

$$f_n^{(\alpha \bmod \delta)}(x) \geq f_n^{(\alpha \bmod \delta)}(1) \cdot \left(\frac{x+1}{2}\right)^{\frac{2 \cdot \phi(\delta n)}{\phi(\delta)}}.$$

Proof. The claim is evident for $x = 1$, and we will show that

$$\frac{f_n^{(\alpha \bmod \delta)}(x)}{(x+1)^{\frac{2 \cdot \phi(\delta n)}{\phi(\delta)}}}$$

is increasing in x. Indeed

$$\frac{f_n^{(\alpha \bmod \delta)}(x)}{(x+1)^{\frac{2 \cdot \phi(\delta n)}{\phi(\delta)}}} = \prod_{a \in (\mathbb{Z}/\delta n)^\times : a \equiv \pm\alpha \pmod{\delta}} \frac{|x - \zeta_n^a|}{x+1},$$

and it suffices to show each factor is increasing in x. But for all $z \in S^1$

$$\frac{|x-z|^2}{(x+1)^2} = \frac{x^2 - 2x \cdot \Re z + 1}{x^2 + 2x + 1} = 1 - \frac{2x}{(x+1)^2} \cdot (1 + \Re z),$$

which is increasing in x because $\frac{x}{(x+1)^2} = \frac{1}{x+1} - \frac{1}{(x+1)^2}$ decreases in x when $x \geq 1$. □

For $a, b \in \mathbb{Z}^+$, write $\gcd(a, b^\infty) := \prod_{p|b} p^{v_p(a)}$, and $\mathrm{rad}(a) := \prod_{p|a} p$.

Lemma 3.9. *Let $n \in \mathbb{Z}^+$. Let $m := \frac{n}{\gcd(n, \delta^\infty)}$. Then*

$$f_n^{(\alpha \bmod \delta)}(1) = \prod_{S \subseteq \{p|m\}} \left|1 - \zeta_\delta^{\alpha \cdot \prod_{p \in S} p^{-1} \pmod{\delta}}\right|^{2 \cdot (-1)^{\#|S|}}.$$

Proof. We first claim that if $\mathrm{rad}\left(\frac{n}{\gcd(n,\delta^\infty)}\right) = \mathrm{rad}\left(\frac{n'}{\gcd(n',\delta^\infty)}\right)$ then $f_n^{(\alpha \bmod \delta)}(1) = f_{n'}^{(\alpha \bmod \delta)}(1)$. This follows by repeatedly applying the following. If $p|n$ is such that $k := v_p(\delta n) \geq 2$, then, writing $\delta n =: p^k \cdot s$, because $X^p - Y^p = \prod_{b \in \mathbb{F}_p} (X - \zeta_p^b \cdot Y)$ as elements of $\mathbb{Z}[\zeta_p][X, Y]$,

$$\begin{aligned} f_n^{(\alpha \bmod \delta)}(1) &= \prod_{a \in (\mathbb{Z}/p^{k-1}s)^\times : a \equiv \pm\alpha \pmod{\delta}} \prod_{b \in \mathbb{F}_p} (1 - \zeta_{p^k \cdot s}^{a + p^{k-1} \cdot s \cdot b}) \\ &= \prod_{a \in (\mathbb{Z}/p^{k-1}s)^\times : a \equiv \pm\alpha \pmod{\delta}} (1 - \zeta_{p^{k-1} \cdot s}^a). \end{aligned}$$

Therefore without changing $f_n^{(\alpha \bmod \delta)}(1)$ we may assume without loss of generality that n is square-free and such that $\gcd(n, \delta) = 1$.

Now if $p|n$, writing $\delta n =: p \cdot n_0$ and letting $p', n_0' \in \mathbb{Z}$ be such that $pp' + n_0 n_0' = 1$,

$$\begin{aligned} f_n^{(\alpha \bmod \delta)}(1) &= \prod_{a \in (\mathbb{Z}/n_0)^\times : a \equiv \pm\alpha \pmod{\delta}} \prod_{b \in \mathbb{F}_p^\times} (1 - \zeta_{pn_0}^{app' + bn_0 n_0'}) \\ &= \prod_{a \in (\mathbb{Z}/n_0)^\times : a \equiv \pm\alpha \pmod{\delta}} \prod_{b \in \mathbb{F}_p^\times} (1 - \zeta_{n_0}^{ap'} \cdot \zeta_p^{bn_0'}) \\ &= \prod_{a \in (\mathbb{Z}/n_0)^\times : a \equiv \pm\alpha \pmod{\delta}} \prod_{b \in \mathbb{F}_p^\times} (1 - \zeta_{n_0}^{ap'} \cdot \zeta_p^{b}) \end{aligned}$$

via $b \mapsto p \cdot b$. Now we apply the identity $\frac{X^p - Y^p}{X - Y} = \prod_{b \in \mathbb{F}_p^\times} (X - \zeta_p^b \cdot Y)$ to find:

$$\begin{aligned} f_n^{(\alpha \bmod \delta)}(1) &= \prod_{a \in (\mathbb{Z}/n_0)^\times : a \equiv \pm\alpha \pmod{\delta}} \frac{(1 - \zeta_{n_0}^{a})}{(1 - \zeta_{n_0}^{ap'})} \\ &= \frac{f_{\frac{n}{p}}^{(\alpha \bmod \delta)}(1)}{f_{\frac{n}{p}}^{(\alpha p' \bmod \delta)}(1)}. \end{aligned}$$

Since the lemma is evident for $n = 1$, by induction on the number of prime factors of n we find that

$$\begin{aligned} f_n^{(\alpha \bmod \delta)}(1) &= \prod_{S \subseteq \{\ell | \frac{n}{p}\}} \left(\frac{\left|1 - \zeta_\delta^{\alpha \cdot \prod_{\ell \in S} \ell^{-1} \pmod{\delta}}\right|}{\left|1 - \zeta_\delta^{\alpha \cdot p^{-1} \cdot \prod_{\ell \in S} \ell^{-1} \pmod{\delta}}\right|} \right)^{2 \cdot (-1)^{\#|S|}} \\ &= \prod_{S \subseteq \{\ell | n\}} \left|1 - \zeta_\delta^{\alpha \cdot \prod_{\ell \in S} \ell^{-1} \pmod{\delta}}\right|^{2 \cdot (-1)^{\#|S|}}, \end{aligned}$$

and we are done. □

Corollary 3.10. *Let $n \in \mathbb{Z}^+$ with $n \geq 3$ be odd. Then*

$$f_n^{(1 \bmod 8)}(1) = \begin{cases} 1 & \exists p | n : p \equiv \pm 1 \pmod 8, \\ (1 + \sqrt{2})^{-2^{\omega(n)}} & \textit{else} \end{cases}$$

and

$$f_n^{(3 \bmod 8)}(1) = \begin{cases} 1 & \exists p | n : p \equiv \pm 1 \pmod 8, \\ (1 + \sqrt{2})^{2^{\omega(n)}} & \textit{else,} \end{cases}$$

whence

$$f_n^{(1 \bmod 8)}(\sqrt{2}) \geq \left(\frac{\sqrt{2}+1}{2}\right)^{2 \cdot \phi(n)} \cdot \begin{cases} 1 & \exists p | n : p \equiv \pm 1 \pmod 8, \\ (1 + \sqrt{2})^{-2^{\omega(n)}} & \textit{else} \end{cases}$$

and

$$f_n^{(3 \bmod 8)}(\sqrt{2}) \geq \left(\frac{\sqrt{2}+1}{2}\right)^{2 \cdot \phi(n)} \cdot \begin{cases} 1 & \exists p | n : p \equiv \pm 1 \pmod 8, \\ (1 + \sqrt{2})^{2^{\omega(n)}} & \textit{else.} \end{cases}$$

Proof. If there is a $p|n$ with $p \equiv \pm 1 \pmod 8$, then pair $S - \{p\}$ with $S \cup \{p\}$ in the conclusion of Lemma 3.9 to see that $f_n^{(1 \bmod 8)}(1) = f_n^{(3 \bmod 8)}(1) = 1$. Otherwise every $p|n$ is such that $p \equiv \pm 3 \pmod 8$, so that by Lemma 3.9

$$f_n^{(1 \bmod 8)}(1) = \left(\frac{|1-\zeta_8|}{|1-\zeta_8^3|}\right)^{2^{\omega(n)}} = (1+\sqrt{2})^{-2^{\omega(n)}}.$$

By the same reasoning

$$f_n^{(3 \bmod 8)}(1) = \left(\frac{|1-\zeta_8^3|}{|1-\zeta_8|}\right)^{2^{\omega(n)}} = (1+\sqrt{2})^{2^{\omega(n)}}.$$

We are done by Lemma 3.8. □

Corollary 3.11. *Let $n \in \mathbb{Z}^+$ with $n \geq 3$ be odd. Let $m := \frac{n}{\gcd(n,6^\infty)}$. Then*

$$f_n^{(1 \bmod 12)}(1) = \begin{cases} 1 & \exists p|m : p \equiv \pm 1 \pmod{12}, \\ (2+\sqrt{3})^{-2^{\omega(m)}} & \textit{else} \end{cases}$$

and

$$f_n^{(5 \bmod 12)}(1) = \begin{cases} 1 & \exists p|m : p \equiv \pm 1 \pmod{12}, \\ (2+\sqrt{3})^{2^{\omega(m)}} & \textit{else,} \end{cases}$$

whence

$$f_n^{(1 \bmod 12)}(\sqrt{3}) \geq \left(\frac{\sqrt{3}+1}{2}\right)^{\frac{\phi(12n)}{2}} \cdot \begin{cases} 1 & \exists p|m : p \equiv \pm 1 \pmod{12}, \\ (2+\sqrt{3})^{-2^{\omega(m)}} & \textit{else} \end{cases}$$

and

$$f_n^{(5 \bmod 12)}(\sqrt{3}) \geq \left(\frac{\sqrt{3}+1}{2}\right)^{\frac{\phi(12n)}{2}} \cdot \begin{cases} 1 & \exists p|m : p \equiv \pm 1 \pmod{12}, \\ (2+\sqrt{3})^{2^{\omega(m)}} & \textit{else.} \end{cases}$$

Proof. If there is a $p|m := \frac{n}{\gcd(n,6^\infty)}$ with $p \equiv \pm 1 \pmod{12}$, then pair $S - \{p\}$ with $S \cup \{p\}$ in the conclusion of Lemma 3.9 to see that $f_n^{(1 \bmod 12)}(1) = f_n^{(5 \bmod 12)}(1) = 1$. Otherwise every $p|m$ is such that $p \equiv \pm 5 \pmod{12}$, so that by Lemma 3.9

$$f_n^{(1 \bmod 12)}(1) = \left(\frac{|1-\zeta_{12}|}{|1-\zeta_{12}^5|}\right)^{2^{\omega(m)}} = (2+\sqrt{3})^{-2^{\omega(m)}}.$$

By the same reasoning

$$f_n^{(5 \bmod 12)}(1) = \left(\frac{|1-\zeta_{12}^5|}{|1-\zeta_{12}|}\right)^{2^{\omega(m)}} = (2+\sqrt{3})^{2^{\omega(m)}}.$$

We are done by Lemma 3.8. □

4. Action on 2-groups and primitivity of local systems

We begin this section with a group theoretic lemma which will be used in the proof of primitivity given in Theorem 4.5.

Lemma 4.1. *Suppose A is a cyclic group of prime order p that acts faithfully on a finite q-group G, where $p \neq q$ are primes. Let n be the order of q modulo p. Let $\chi \in \mathrm{Irr}(G)$ be A-invariant and faithful, and write $\chi(1) = q^a$. Then $n \leq 2a$.*

Proof. We argue by induction on $|G|$. Let $C = \mathbf{C}_G(A) < G$. Let $C \leq N < G$ be maximal A-invariant in G. Since G is nilpotent, $N \lhd G$. Also, G/N is an irreducible A-module. Notice that A cannot act trivially on G/N, because $G = [G, A]C$, by coprime action. Hence, G/N is a faithful irreducible $\mathbb{F}_q[A]$-module. By [MW, Example 2.7], say, $|G/N| = q^n$. Let $\theta \in \mathrm{Irr}(N)$ be A-invariant under χ; such exists by [Is3, Theorem 13.27]. Now, since G/N is an abelian chief factor of the semidirect product GA and χ is GA-invariant, by the Isaacs "going down" theorem [Is3, Theorem 6.18], either $\chi_N = \theta$, or $\chi_N = e\theta$ with $e^2 = |G/N|$, or $\theta^G = \chi$.

In the third case, $\chi(1) = q^n\theta(1) = q^{n+b} = q^a$, for some $b \geq 0$. Thus $n \leq n + b = a \leq 2a$. In the second case, q^n is a square, and that $\chi(1)/\theta(1) = q^{n/2}$. Then $\chi(1) = q^{\frac{n}{2}+c} = q^a$, for some $c \geq 0$. Then $a = \frac{n}{2} + c$, and again $n \leq 2a$.

In the first case, $\chi_N = \theta \in \mathrm{Irr}(N)$. If A does not act trivially on N, then A acts faithfully on N. Since θ is A-invariant and faithful, then we are done by the inductive hypothesis. Otherwise, A acts trivially on N, and therefore $N = \mathbf{C}_G(A)$ (because N is maximal A-invariant). By [N2, Lemma 2.1], $[G, A] \subseteq \mathrm{Ker}(\chi)$. Since χ is faithful, A acts trivially on G. But this cannot happen. □

We will now introduce a general class of Airy sheaves $\mathcal{F}(q, f)$ that includes the sheaves $\mathcal{F}_q$. Recall that $q = 2^{2n+1} = 2q_0^2$ and $t(q) := q - 2q_0 + 1$. Let $k_0/\mathbb{F}_2$ be a finite extension, and $f(x) \in k_0[x]$ a polynomial of degree $(1 + q_0)t(q)$. Form the Artin-Schreier-Witt lisse sheaf

$$\mathcal{L}(q, f) := \mathcal{L}_{\psi_2([x^{t(q)}, f(x)])}$$

on $\mathbb{A}^1/k_0$. Then $\mathcal{F}(q, f)$ is the constant field twisted Fourier transform

$$\mathcal{F}(q, f) := \mathrm{FT}_\psi(\mathcal{L}(q, f)) \otimes (1 - (-1)^n i)^{-\deg}. \tag{4.1.1}$$

The trace function of $\mathcal{F}(q, f)$ at $t \in k$, k/k_0 a finite extension, is

$$t \mapsto \frac{-1}{\big((1 - (-1)^n\, i\big)^{\deg(k/\mathbb{F}_2)}} \sum_{x \in k} \psi_2(\mathrm{Trace}_{W_2(k)/W_2(\mathbb{F}_2)}([x^{t(q)}, f(x) + tx])). \tag{4.1.2}$$

Assume in addition that

$$f(x) = f_1(x^{t(q)}) \tag{4.1.3}$$

for some polynomial $f_1(x) \in k_0[x]$ of degree $1 + q_0$. If we make the substitution $x \mapsto x/t$, then (4.1.2) for $t \in k^\times$ becomes

$$t \mapsto \frac{-1}{\big(1 - (-1)^n\, i\big)^{\deg(k/\mathbb{F}_2)}} \sum_{x \in k} \psi_2\big(\mathrm{Trace}_{W_2(k)/W_2(\mathbb{F}_2)}([x^{t(q)}/t^{t(q)}, f_1(x^{t(q)}/t^{t(q)}) + x])\big),$$

For

$$t(q) = rs,$$

we get a descent $\mathcal{G}(q, f, r)$ of $\mathcal{F}(q, f)$ to $\mathbb{G}_m/k_0$ whose trace function is now

$$t \mapsto \frac{-1}{\big(1 - (-1)^n\, i\big)^{\deg(k/\mathbb{F}_2)}} \sum_{x \in k} \psi_2\big(\mathrm{Trace}_{W_2(k)/W_2(\mathbb{F}_2)}([x^{t(q)}/t^s, f_1(x^{t(q)}/t^s) + x])\big),$$

and whose Kummer pullback by r^{th} power is (the restriction to $\mathbb{G}_m/k_0$ of) $\mathcal{F}(q, f)$:

$$[r]^\star\mathcal{G}(q, f, r) \cong \mathcal{F}(q, f)|\mathbb{G}_m.$$

We next give a key lemma of Šuch, which is proved in [Such, Proposition 11.1] but not stated there explicitly.

Lemma 4.2. (Šuch) *Let $\mathcal{F}$ be an Airy sheaf of rank $n \geq 2$ on $\mathbb{A}^1/\overline{\mathbb{F}_p}$, i.e. $\mathcal{F}$ is the Fourier transform $\mathrm{FT}(\mathcal{L})$ of a lisse, rank one sheaf $\mathcal{L}$ on $\mathbb{A}^1/\overline{\mathbb{F}_p}$ with $\mathsf{Swan}_\infty(\mathcal{L}) = n+1$. If $\mathcal{F}$ is induced, then it is induced from an Artin-Schreier covering of $\mathbb{A}^1/\overline{\mathbb{F}_p}$. In particular, if $\mathcal{F}$ is induced, then it is induced from a normal subgroup of index p of its G_{geom}.*

Proof. Let us recall the argument, which is contained in the proof of [Such, Proposition 11.1]. If $\mathcal{F}$ is induced, then it is $g_\star\mathcal{H}$, in which case

$$\mathrm{End}(\mathcal{F}) = (g_\star\mathcal{H}) \otimes (g_\star\mathcal{H}^\vee) \supseteq g_\star(\mathcal{H} \otimes \mathcal{H}^\vee) \supseteq g_\star\mathbb{1},$$

and hence $\mathrm{End}^0(\mathcal{F}) \supseteq g_\star\mathbb{1}/\mathbb{1}$. But $g_\star\mathbb{1}/\mathbb{1}$ has rank $< n$, and all its slopes are $\leq (n+1)/n = 1+1/n$. But each slope of $g_\star\mathbb{1}/\mathbb{1}$ has denominator in lowest terms at most the rank of $g_\star\mathbb{1}/\mathbb{1}$, which is $< n$. Therefore each slope, being at most $1+1/n$, is in fact ≤ 1. Then by [Such, Corollary 3.3], $g_\star\mathbb{1}/\mathbb{1}$ is the direct sum of various $\mathcal{L}_{\psi(ax)}$.

The rest of the argument is given in the first eight lines of the second paragraph of the proof of [Such, Proposition 11.1]. □

We will need the following general result, a slight generalization of [KT1, Theorem 4.6].

Theorem 4.3. *Let $\mathcal{F}$ be a semisimple lisse sheaf on $\mathbb{G}_m/\overline{\mathbb{F}_p}$ which is tame at 0. Denote by J the image of $I(\infty)$ in $G := G_{\mathrm{geom},\mathcal{F}}$. Then G is the Zariski closure of the normal subgroup of G generated by all G-conjugates of J.*

Proof. Denote by G_∞ this Zariski closure. Then G is reductive, and hence its quotient G/G_∞ is reductive. It suffices to show that every irreducible representation of G/G_∞ is trivial. But a d-dimensional irreducible representation is a lisse sheaf of rank d on $\mathbb{G}_m/\overline{\mathbb{F}_p}$ which is tame at 0 (because $P(0)$ dies in G) and lisse at ∞. By multiplicative inversion, this is an irreducible local system on $\mathbb{A}^1/\overline{\mathbb{F}_p}$ which is tame at ∞, so a representation of $\pi_1^{\mathrm{tame}}(\mathbb{A}^1/\overline{\mathbb{F}_p})$, which is the trivial group. □

We will also need a very special case (about subgroups of index 2) of (the second part of) the following proposition. Since we cannot find a reference for it, we give a proof.

Proposition 4.4. (i) *Let G be a Lie group and H an abstract subgroup of finite index in G. Then H is closed.*

(ii) *Let G be a reductive linear algebraic group over an algebraically closed field k, and let H be an abstract subgroup of finite index in G. Then H is Zariski closed.*

Proof. (a) We give a proof of statement (i), which is due to Jason DeVito, posted on `MathStackExchange`.

(a1) First we show that if G is connected, then G is generated by its divisible subgroups. Indeed, there is an open set $U \subseteq G$ containing the identity such that $U \subseteq \exp(\mathcal{L})$ for the Lie algebra $\mathcal{L}$ of G. For any u in U, if $u = \exp(X)$, then u lies in the divisible subgroup $\{\exp(tX) \mid t \in \mathbb{R}\}$ of G. Since G is generated by U, the claim follows.

(a2) Next we show that if G is connected and $H \leq G$ is of finite index, then $H = G$. Indeed, by considering the action via left translation of G on the finite set G/H of left H-cosets, we see that H contains a normal subgroup $K \lhd G$ of finite index. By (i), G, and so G/K, is generated by its divisible subgroups. But G/K is finite, so $K = G$.

(a3) In the general case, consider the map $\iota : G^\circ/(H \cap G^\circ) \to G/H$ defined by $x(H \cap G^\circ) \mapsto xH$. Then ι is injective, and so $H \cap G^\circ$ has finite index in G°. By (a2), $H \geq G^\circ$, and so H is a union of a finite number of G°, each of which is closed. Hence H is closed.

(b) For statement (ii), the argument in (a3) shows that it suffices to prove that if G is connected reductive and H has finite index in G, then $H = G$. The argument in (a2) allows us to further assume that $H \lhd G$. Recall [C, p. 16] that $G = T[G, G]$, where $T = \mathbf{Z}(G)^\circ$ is a central torus of G, and the derived subgroup $[G, G]$ is a central product $G_1 \circ \ldots \circ G_n$ of simple groups. In particular, for each i, $H \cap G_i$ is a normal (abstract) subgroup of finite index of G_i. As G_i is generated by (unipotent) root subgroups, [Tits, Main Theorem] implies that $H \cap G_i$ is either equal to G_i or contained in $\mathbf{Z}(G_i)$. The finite index assumption now ensures that $H \geq G_i$ for all i, and thus $H \geq [G, G]$. Next, $H \cap T$ is a normal (abstract) subgroup of finite index say m in T. In particular, H contains t^m for all $t \in T$. But the torus T is $(k^\times)^r$ for some r, so $k = \overline{k}$ implies that any element in T is an m^{th} power, and hence $H \geq T$, completing the proof. [The referee kindly pointed out a much simpler argument as follows. If $H \lhd G$ has index N in G then G contains all powers g^N, $g \in G$. But G, being connected reductive, is generated by its maximal tori, and the map $g \mapsto g^N$ is surjective on each maximal torus. Hence $H = G$.] □

As pointed out by the referee, in both of the cases of Proposition 4.4, once H is closed, it is also open (indeed, $G \smallsetminus H$ is a disjoint union of a finite number of cosets gH, each being closed, and so it is closed).

Theorem 4.5. *Let $q = 2^{2n+1}$ with $n \in \mathbb{Z}_{\geq 1}$ and $n \neq 2$. Under the assumption* (4.1.3)*, the group $G_{\text{geom},\mathcal{F}(q,f)}$ of the Airy sheaf $\mathcal{F}(q, f)$ has no subgroups of index* 2*. As a consequence, the Airy sheaf $\mathcal{F}(q, f)$ is not geometrically induced, and hence none of the sheaves $\mathcal{G}(q, f, r)$ is geometrically induced.*

Proof. Assume to the contrary that the Airy sheaf $\mathcal{F}(q, f)$ is induced. Then, by Lemma 4.2, the underlying representation V of the geometric monodromy group $G := G_{\text{geom}}$ of $\mathcal{F}(q, f)$ is induced from a subgroup G_1 of G of index 2.

(i) For each divisor $r > 1$ of $t(q)$, consider the descent $\mathcal{G}(q, f, r)$. Because $\mathcal{F}(q, f)$ is lisse at 0, the image of $I(0)$ in the geometric monodromy group H of $\mathcal{G}(q, f, r)$ is the cyclic group $\mu_r(\overline{\mathbb{F}_2})$ of order r. Because the ∞-slopes of $\mathcal{F}(q, f)$ are $\dfrac{(2^n+1)t(q)}{(2^n+1)t(q)-1}$, if $r > 1$, then the ∞-slopes of $\mathcal{G}(q, f, r)$ are $(1/r)\dfrac{(2^n+1)t(q)}{(2^n+1)t(q)-1} < 1$. It then follows from [KT1, Proposition 4.2] that H is equal to the Zariski closure H_0^{Zar} in H of the normal closure H_0 in H of the image of $I(0)$.

We next show that for $r > 1$, H has no subgroup of index 2. We argue by contradiction. Suppose that H has a subgroup H_1 of index 2. Since every H-conjugate of the image of $I(0)$ has odd order r, all such conjugates are contained in H_1, and thus $H_0 \leq H_1$. But H_1 is closed in H by Proposition 4.4(ii), so $H = H_0^{\text{Zar}} \leq H_1$, and hence $H = H_1$, a contradiction. We have shown that H has no subgroup of index 2.

(ii) We also know that G is a normal subgroup of H of index dividing r, simply because by the r^{th} power map, $\mathbb{G}_m/\overline{\mathbb{F}_2}$ becomes a finite étale Galois covering of itself with cyclic group of order r, and G and H are respectively the Zariski closure of the images of $\pi_1(\mathbb{G}_m/\overline{\mathbb{F}_2})$ and of a normal subgroup of cyclic index r of that group. Now if $H = G$, then the existence of G_1 leads to a contradiction by (i). If we now take r to be a prime dividing $t(q)$, then $H/G \cong C_r$.

Let J and Q denote the images of $I(\infty)$ and of $P(\infty)$ in H. By Theorem 4.3, H is equal to the Zariski closure H_∞^{Zar} in H of the normal closure H_∞ in H of J. Suppose for the moment that $r \nmid |J|$. Then every H-conjugate of J has order coprime to r, and so they are all contained in G, and thus $H_\infty \leq G$. But G is closed in H, so $H_\infty^{\text{Zar}} \leq G$, and hence $H = G$, a contradiction.

We have shown that r divides $|J|$. Recall that $J = Q \rtimes C$, with C a cyclic $2'$-group that permutes cyclically and transitively the $q-1$ simple Q-submodules V_i in V, each of dimension $q_0 = 2^n$. As Q is a 2-group, C is of order divisible by r.

(iii) Since $n \neq 2$, by Theorem 3.4 the integer $t(q) = q - \sqrt{2q} + 1$ admits a prime divisor

$$r = \mathrm{ppd}(2, 4(2n+1)). \tag{4.5.1}$$

At this point, we take for r a $\mathrm{ppd}(2, 4(2n+1))$ which divides $t(q)$. Fix $c \in C$ of order r. Since $r|t(q)$, $r \nmid (q-1)$, and so c stabilizes each of the subspace V_i, and certainly normalizes Q. For each i, let Φ_i denote the representation of $\langle Q, c\rangle$ on V_i. We claim that $\Phi_i(c)$ centralizes $\Phi_i(Q)$. Otherwise, $\Phi_i(c)$ acts faithfully on $\Phi_i(Q)$, of prime order r, and $\Phi_i(Q)$ is faithful and irreducible of degree 2^n. Hence by Lemma 4.1, the order of 2 modulo r is at most $2n$, which contradicts (4.5.1).

Therefore, for each i, $\Phi_i(c) = \alpha_i \cdot \mathrm{Id}_{V_i}$ for some $\alpha_i \in \mathbb{C}^\times$. But the cyclic group C permutes the V_i's transitively and $c \in C$, so $\alpha_1 = \ldots = \alpha_{q-1} =: \alpha$, i.e. c acts on V as $\alpha \cdot \mathrm{Id}_V$. As $|c| = r$, $\alpha \neq 1$ is a primitive r^{th} root of unity. Thus we may assume that $c \in J$ has trace $\dim(V) \cdot \zeta_r$. On the other hand, by Theorem 2.2 and (4.1.2), the trace of every element in J belongs to $\mathbb{Q}(i)$. Thus $\zeta_r \in \mathbb{Q}(i)$, a contradiction since r is an odd prime.

(iii) Since the irreducible representation V of $G = G_{\mathrm{geom}}$ of $\mathcal{F}(q, f)$ is not induced, for any $r|t(q)$, the representation of G_{geom} of $\mathcal{G}(q, f, r)$ on V, which contains G, is not induced. □

5. Condition (**S**+) and autoduality for Airy sheaves

In this section, we continue to consider Airy sheaves $\mathcal{F}(q, f)$ of the same general shape (4.1.1), but we consider them only geometrically, i.e. as lisse sheaves on $\mathbb{A}^1/\overline{\mathbb{F}_2}$. The key insight on which the results of this section are based is due to Šuch, cf. [Such, Proposition 11.1].

Lemma 5.1. (Šuch) *Let $\mathcal{F}$ be an Airy sheaf of rank $D \geq 2$ on $\mathbb{A}^1/\overline{\mathbb{F}_p}$. Let $\mathcal{H}$ be a direct factor of $\mathrm{End}(\mathcal{F})$ of rank $r < D$. Then $\mathcal{H}$ is a direct sum of $\mathcal{L}_{\psi(ax)}$ for various $a \in \overline{\mathbb{F}_p}$.*

Proof. The ∞-slopes of $\mathcal{F}$ are all $1 + 1/D$. All slopes of $\mathrm{End}(\mathcal{F})$ are therefore $\leq 1 + 1/D$. Thus all slopes of $\mathcal{H}$ are $\leq 1 + 1/D$. But each slope of $\mathcal{H}$, written in lowest terms, has denominator $\leq r$. Therefore $\mathcal{H}$ has all slopes ≤ 1. Now take an irreducible constituent $\mathcal{K}$ of $\mathcal{H}$. Its Fourier transform, i.e. $t \mapsto H_c(A^1/\overline{\mathbb{F}_p}, \mathcal{K} \otimes \mathcal{L}_{\psi(tx)})$, is perverse irreducible on $A^1/\overline{\mathbb{F}_p}$, so is either a single delta function δ_a or is the extension by direct image of a lisse sheaf on a dense open set. But on a dense open set of the t-line, $\mathcal{K} \otimes \mathcal{L}_{\psi(tx)}$ has all ∞-slopes 1, so $H^2_c(A^1/\overline{\mathbb{F}_p}, \mathcal{K} \otimes \mathcal{L}_{\psi(tx)}) = 0$ and by the Euler-Poincaré formula $\chi_c(A^1/\overline{\mathbb{F}_p}, \mathcal{K} \otimes \mathcal{L}_{\psi(tx)}) = 0$, so $\mathrm{FT}(\mathcal{K})$ is punctual, hence a single δ_a. This means in turn that each irreducible constituent of $\mathcal{H}$ is an $\mathcal{L}_{\psi(ax)}$. Because $\mathcal{F}$ is irreducible, $\mathrm{End}(\mathcal{F})$ is completely reducible, hence $\mathcal{H}$ is completely reducible, and so it is the sum of its irreducible constituents. □

Theorem 5.2. *Let $\mathcal{F}$ be an Airy sheaf of rank at least 2 on $\mathbb{A}^1/\overline{\mathbb{F}_p}$. Then the following conditions are equivalent.*

(i) *$\mathcal{F}$ is geometrically induced.*
(ii) *$\mathrm{End}(\mathcal{F})$ contains a summand $\mathcal{L}_{\psi(ax)}$ for some $a \neq 0$ in $\overline{\mathbb{F}_p}$.*
(iii) *There exists a geometric isomorphism $\mathcal{F} \cong \mathcal{F} \otimes \mathcal{L}_{\psi(-ax)}$ for some $a \neq 0$ in $\overline{\mathbb{F}_p}$.*

Proof. Let us denote by n the rank of $\mathcal{F}$. If $\mathcal{F}$ is induced, then it is $g_\star\mathcal{H}$, in which case

$$\mathrm{End}(\mathcal{F}) = (g_\star\mathcal{H}) \otimes (g_\star\mathcal{H}^\vee) \supseteq g_\star(\mathcal{H} \otimes \mathcal{H}^\vee) \supseteq g_\star\mathbb{1},$$

and hence $\mathrm{End}^0(\mathcal{F}) \supseteq g_\star\mathbb{1}/\mathbb{1}$. But $g_\star\mathbb{1}/\mathbb{1}$ has rank less than n. So by Lemma 5.1, $g_\star\mathbb{1}/\mathbb{1}$ is the direct sum of various $\mathcal{L}_{\psi(ax)}$. As $\mathrm{End}^0(\mathcal{F})$ does not contain the trivial sheaf (by irreducibility of $\mathcal{F}$), we find that $\mathrm{End}^0(\mathcal{F})$, and hence $\mathrm{End}(\mathcal{F})$, contains some $\mathcal{L}_{\psi(ax)}$ for some nonzero $a \in \overline{\mathbb{F}_2}$.

Conversely, suppose $\mathrm{End}(\mathcal{F})$ contains a summand $\mathcal{L}_{\psi(ax)}$ for some $a \neq 0$ in $\overline{\mathbb{F}_p}$. Thus there is a nonzero geometric homomorphism from $\mathcal{F}$ to $\mathcal{F} \otimes \mathcal{L}_{\psi(-ax)}$. But source and target are geometrically isomorphic, so every nonzero homomorphism is an isomorphism. Thus we have a geometric isomorphism

$$\mathcal{F} \cong \mathcal{F} \otimes \mathcal{L}_{\psi(-ax)}.$$

That $\mathcal{F}$ is geometrically induced is the special case, where G is G_{geom} for $\mathcal{F} \oplus \mathcal{L}_{\psi(-ax)}$, V is $\mathcal{F}$, L is $\mathcal{L}_{\psi(-ax)}$, N is p, and $\mathbb{E}$ is $\overline{\mathbb{Q}_\ell}$, of the following general statement in characteristic zero representation theory. □

Theorem 5.3. *Over an algebraically closed field $\mathbb{E}$ of characteristic zero, let V be a finite dimensional irreducible representation of dimension $d \geq 2$ of a group G, and L a one-dimensional representation of G which, viewed as a linear character χ of G, has finite order $N > 1$. Suppose that $V \cong V \otimes L$ as representations of G. Denote by $G_0 := \mathrm{Ker}(\chi)$ the kernel of χ, so that $G_0 \lhd G$ with G/G_0 cyclic of order N. Then V is induced from a representation of a subgroup H with $G_0 \leq H < G$.*

Proof. We first reduce to the case when N is prime. If $V \cong V \otimes L$, then by induction $V \cong V \otimes L^{\otimes n}$ for every integer n. Let r be a prime dividing N. Replacing L by $L^{\otimes(N/r)}$ and $\mathrm{Ker}(\chi)$ by the overgroup $K := \mathrm{Ker}(\chi^{(N/r)})$, we are reduced to the case when $N = r$ is prime.

Let U be a simple summand of $V|_K$, which is semisimple since $K \lhd G$. By Clifford theory, cf. [CR1, (50.5)], V is induced so long as $V|_K$ is not isotypic. Hence, if V is not induced, then $V|_K \cong eU := \underbrace{U \oplus U \oplus \ldots \oplus U}_{e \text{ times}}$ for some $e \in \mathbb{Z}_{\geq 1}$. Note that $\mathrm{Ind}_K^G(\mathbb{E}) \cong \oplus_{i=1}^r L^{\otimes i}$, so by Frobenius reciprocity, cf. [CR2, (10.20)],

$$\mathrm{Ind}_K^G(V|_K) \cong \mathrm{Ind}_K^G\big((V|_K) \otimes \mathbb{E}\big) \cong V \otimes \mathrm{Ind}_K^G(\mathbb{E}) \cong \oplus_{i=1}^r (V \otimes L^{\otimes i}) \cong rV.$$

Again by Frobenius reciprocity [CR2, (10.8)],

$$e^2 = \dim \mathrm{Hom}_K(V|_K, V|_K) = \dim \mathrm{Hom}_G\big(V, \mathrm{Ind}_K^G(V|_K)\big) = \dim \mathrm{Hom}_G(V, rV) = r,$$

a contradiction as r is a prime. □

The following general result is stated for ease of later reference.

Theorem 5.4. *Let $\mathcal{F}$ be a lisse irreducible $\overline{\mathbb{Q}_\ell}$-sheaf of rank $d \geq 2$ on a smooth, geometrically connected $X/\overline{\mathbb{F}_p}$. Suppose that $\mathrm{End}^0(\mathcal{F})$ contains a rank one summand $\mathcal{L}$. Then $\mathcal{F}$ is induced.*

Proof. Because $\mathcal{L}$ occurs in $\mathrm{End}^0(\mathcal{F})$, it cannot be trivial (as by irreducibility of $\mathcal{F}$, $\mathrm{End}(\mathcal{F})$ contains $\mathbb{1}$ exactly once). Exactly as in the proof of the implication (ii) $\implies$ (iii) in Theorem 5.2, we infer that $\mathcal{F} \cong \mathcal{F} \otimes \mathcal{L}^{-1}$. Taking determinants of this isomorphism, we find that $\mathcal{L}^{\otimes d}$ is trivial. Thus $\mathcal{L}$ has finite order $N > 1$ as a character of $\pi_1(X)$. Now apply Theorem 5.3. □

Theorem 5.5. *Let $k_0/\mathbb{F}_2$ be a finite extension, and $f(x) \in k_0[x]$ a polynomial of degree $(1+q_0)t(q)$. Then the Airy sheaf $\mathcal{F}(q, f)$ introduced in (4.1.1) is geometrically primitive, i.e. is not geometrically induced.*

Proof. (i) In view of Theorem 5.2, it suffices to show that there is no geometric isomorphism from $\mathcal{F}(q, f)$ to $\mathcal{F}(q, f) \otimes \mathcal{L}_{\psi(ax)}$ for any $a \neq 0$ in $\overline{\mathbb{F}_p}$. We argue by contradiction. Because $\mathcal{F}(q, f)$ was geometrically a Fourier transform, so is $\mathcal{F}(q, f) \otimes \mathcal{L}_{\psi(ax)}$; the effect of tensoring with $\mathcal{L}_{\psi(ax)}$ after FT is the same as translating additively by $-a$ before FT:

$$\mathcal{F}(q, f) \otimes \mathcal{L}_{\psi(ax)} = \mathrm{FT}([x \mapsto x - a]^\star \mathcal{L}(q, f)).$$

Since FT is invertible, an isomorphism of $\mathcal{F}(q,f)$ with $\mathcal{F}(q,f)\otimes\mathcal{L}_{\psi(ax)}$ gives an isomorphism of $\mathcal{L}(q,f)$ with its additive translate by $-a$:

$$\mathcal{L}_{\psi_2([x^{t(q)},f(x)])}\cong\mathcal{L}_{\psi_2([(x-a)^{t(q)},f(x-a)])}.$$

We will show no such isomorphism exists.

(ii) Suppose that $n\geq 2$. In this case, we argue as follows. If two lisse rank one sheaves are isomorphic, then so are their tensor squares.

Quite generally, addition of Witt vector of length 2 over an $\mathbb{F}_2$-algebra is given by

$$[a,b]+[A,B]=[a+A,B+b+aA],\ [a,b]+[a,b]=[0,a^2].$$

Thus

$$\mathcal{L}^{\otimes 2}_{\psi_2([g(x),f(x)])}=\mathcal{L}_{\psi_2([g(x),f(x)]+[g(x),f(x)])}=\mathcal{L}_{\psi_2([0,g(x)^2])}=\mathcal{L}_{\psi(g(x)^2)}\cong\mathcal{L}_{\psi(g(x))}.$$

So we would have a geometric isomorphism

$$\mathcal{L}_{\psi(x^{t(q)}))}\cong\mathcal{L}_{\psi((x-a)^{t(q)}))},$$

or equivalently a geometric isomorphism

$$\mathcal{L}_{\psi((x-a)^{t(q)}-x^{t(q)})}\cong\overline{\mathbb{Q}_\ell}.$$

Now we use the explicit shape of $t(q)=q+1-2q_0=2q_0^2-2q_0+1=(q_0-1)(2q_0)+1$.

The key point is that $t(q)=1+dQ$ with $d\geq 2$ prime to $p=2$ (here $d=q_0-1$) and Q a strictly positive power of $p=2$ (here $Q=2q_0$). Then

$$\begin{aligned}(x-a)^{1+qD}&=(x-a)(x^Q-a^Q)^d\\&=(x-a)\big(x^{dQ}-da^Qx^{(d-1)Q}+(\text{terms of degree }\leq(d-2)Q)\big)\\&=x^{1+dQ}-da^Qx^{1+(d-1)Q}+(\text{terms of degree }\leq 1+(d-2)Q)\\&\quad+(\text{polynomial in }x^Q\text{ of degree }d).\end{aligned}$$

Thus up to Artin-Schreier equivalence,

$$(x-a)^{1+dQ}-x^{1+dQ}=-da^Qx^{1+(d-1)Q}+(\text{terms of degree }\leq 1+(d-2)Q)+(\text{a term of degree }d).$$

Thus $\mathcal{L}_{\psi((x-a)^{1+dQ}-x^{1+dQ})}$ has $\mathsf{Swan}=1+(d-1)Q>0$, so is not geometrically trivial.

(iii) We now turn to the case $n=1$, which requires a more delicate analysis. What makes the $n\geq 2$ case argument work is that $q_0-1=2^n-1$ has $n\geq 2$ binary digits. In the $n=1$ case, $t(8)=5$, so the above argument would involve examining

$$(x-a)^5-x^5=(x-a)(x^4-a^4)-x^5=ax^4-a^4x+a^5,$$

but this is Artin-Schreier equivalent to $(a^{1/4}-a^4)x$, which for $a\in\mu_{15}$ is Artin-Schreier trivial.

Thus we must look instead at

$$\mathcal{L}_{\psi_2([(x-a)^5,f(x-a)])}\otimes\mathcal{L}^{-1}_{\psi_2([x^5,f(x)])}=\mathcal{L}_{\psi_2([(x-a)^5,f(x-a)]-[x^5,f(x)])}.$$

Here $-[a,b]=[a,b-a^2]$, implying $-[x^5,f(x)]=[x^5,f(x)-x^{10}]$, so this is

$$\mathcal{L}_{\psi_2([(x-a)^5+x^5,f(x-a)+f(x)-x^{10}+x^5(x-a)^5])}.$$

But $f(x)$ has degree 15, say $f(x)=bx^{15}+cx^{14}+dx^{13}+\text{lower terms}$ with $b\neq 0$. So under Artin-Schreier equivalence

$$f(x)\equiv bx^{15}+dx^{13}+\text{lower terms}.$$

Similarly, under Artin-Schreier equivalence

$$f(x-a)\equiv b(x-a)x^{15}+d(x-a)^{13}+\text{lower terms}.$$

Thus under Artin-Schreier equivalence

$$f(x-a)+f(x)-x^{10}+x^5(x-a)^5 \equiv b(x-a)^{15}-bx^{15}+\text{lower terms.}$$

The difference

$$b(x-a)^{15}-bx^{15} = -abx^{14}+ba^2x^{13}+\text{lower terms}$$

is thus Artin-Schreier equivalent to

$$ba^2x^{13}+\text{lower terms.}$$

Now view $\mathcal{L}_{\psi_2([(x-a)^5+x^5, f(x-a)+f(x)-x^{10}+x^5(x-a)^5])}$ as the tensor product (using $[a,b]=[a,0]+[0,b]$)

$$\mathcal{L}_{\psi_2([(x-a)^5+x^5,0]} \otimes \mathcal{L}_{\psi(f(x-a)+f(x)-x^{10}+x^5(x-a)^5)}.$$

The first factor has $\mathsf{Swan}_\infty \leq 2\times 4$, while the second factor, which is $\mathcal{L}_{\psi(\text{a polynomial of degree 13})}$, has $\mathsf{Swan}_\infty = 13$, and hence their tensor product has $\mathsf{Swan}_\infty = 13$, so is not geometrically trivial. □

Recall that a lisse sheaf $\mathcal{H}$ is *Lie-irreducible* if, in the underlying representation of its G_{geom}, the identity component G°_{geom} acts irreducibly. It is *Lie-self-dual* if the given representation of G_{geom}, when restricted to G°_{geom}, is self-dual.

Theorem 5.6. *Suppose that a lisse sheaf $\mathcal{F}(q,f)$ as in* (4.1.1) *is Lie-irreducible and Lie-self-dual. Then $\mathcal{F}(q,f)$ is self-dual.*

Proof. The two sheaves $\mathcal{F}(q,f)$ and its dual $\mathcal{F}(q,f)^\vee$ are irreducible representations of G_{geom} whose restrictions to the identity component G°_{geom} are isomorphic. So the two, as representations of G_{geom}, differ by a linear character of $G_{\text{geom}}/G^\circ_{\text{geom}}$. Thus

$$\mathcal{F}(q,f)^\vee \cong \mathcal{F}(q,f)\otimes\mathcal{L}$$

for some lisse, rank one $\mathcal{L}$ on $\mathbb{A}^1$. Both $\mathcal{F}(q,f)^\vee$ and $\mathcal{F}(q,f)$ have all ∞-slopes $1+1/\text{rank}(\mathcal{F}(q,f)) < 2$. Therefore $\mathsf{Swan}_\infty(\mathcal{L}) \leq 1$ (otherwise $\mathcal{F}(q,f)^\vee$ would have all ∞-slopes ≥ 2).

If $\mathsf{Swan}_\infty(\mathcal{L})=0$, then $\mathcal{L}$ is lisse on $\mathbb{A}^1$ and tame at ∞, so geometrically trivial, and $\mathcal{F}(q,f)$ is geometrically self-dual. If $\mathsf{Swan}_\infty(\mathcal{L})=1$, then $\mathcal{L}$ is $\mathcal{L}_{\psi(ax)}$ for some nonzero $a\in\overline{\mathbb{F}_p}$. We will show that this case cannot arise.

Recall that $\mathcal{F}(q,f) := \text{FT}_\psi(\mathcal{L}_{\psi_2([x^{t(q)},f(x)])})$. In general, the interaction of FT with duality is a geometric isomorphism

$$D(\text{FT}_\psi(\mathcal{H})) \cong \text{FT}_{\overline{\psi}}(D\mathcal{H})).$$

In characteristic 2, where ψ takes values ± 1, we have $\overline{\psi}=\psi$. Thus

$$\mathcal{F}(q,f)^\vee \cong \text{FT}_\psi(\mathcal{L}_{\psi_2(-[x^{t(q)},f(x)])}) = \text{FT}_\psi(\mathcal{L}_{\psi_2([x^{t(q)},f(x)+(x^{t(q)})^2])})$$

while

$$\mathcal{F}(q,f)\otimes\mathcal{L}_{\psi(ax)} \cong \text{FT}_\psi([x\mapsto x-a]^\star\mathcal{L}_{\psi_2([x^{t(q)},f(x)])} = \text{FT}_\psi(\mathcal{L}_{\psi_2([(x-a)^{t(q)},f(x-a)])}).$$

By Fourier inversion, this is equivalent to a geometric isomorphism

$$\mathcal{L}_{\psi_2([x^{t(q)},f(x)+(x^{t(q)})^2])} \cong \mathcal{L}_{\psi_2([(x-a)^{t(q)},f(x-a)])}.$$

We first treat the case $n\geq 2$. Already the tensor squares of these two lisse rank one sheaves are not geometrically isomorphic, by the identical argument used to treat the case $n\geq 2$ in the proof of Theorem 5.5.

In the case $n=1$, we must show that the lisse rank one sheaf

$$\mathcal{L}_{\psi_2([(x-a)^s,f(x-a)])}\otimes(\mathcal{L}_{\psi_2([x^5,f(x)+(x^5)^2])})^{-1}$$

is not geometrically trivial. The second tensor factor is

$$(\mathcal{L}_{\psi_2([x^5],f(x)+(x^5)^2])})^{-1} = \mathcal{L}_{\psi_2(-[x^5,f(x)+(x^5)^2])} = \mathcal{L}_{\psi_2([x^5,f(x)])}.$$

So we must show that

$$\begin{aligned}\mathcal{L}_{\psi_2([(x-a)^5,f(x-a)])} \otimes \mathcal{L}_{\psi_2([x^5],f(x)])} &= \mathcal{L}_{\psi_2([(x-a)^5,f(x-a)]+[x^5,f(x)])} \\ &= \mathcal{L}_{\psi_2([(x-a)^5+x^5,f(x-a)+f(x)+x^5(x-a)^5])} \\ &= \mathcal{L}_{\psi_2([(x-a)^5+x^5,0])} \otimes \mathcal{L}_{\psi(f(x-a)+f(x)+x^5(x-a)^5)}\end{aligned}$$

is not geometrically trivial. Exactly as in the proof of the $n = 1$ case of Theorem 5.5, the first factor has $\mathsf{Swan}_\infty \leq 2 \times 4 = 8$, while the second factor has $\mathsf{Swan}_\infty = 13$. □

Theorem 5.7. *No sheaf $\mathcal{F}(q, f)$ introduced in* (4.1.1) *is geometrically self-dual.*

Proof. Recall that $\mathcal{F}(q, f) := \mathrm{FT}_\psi\big(\mathcal{L}_{\psi_2([x^{t(q)},f(x)])}\big)$. In general, the interaction of the Fourier transform FT with the duality functor $D(\cdot)$ is a geometric isomorphism

$$D(\mathrm{FT}_\psi(\mathcal{H})) \cong \mathrm{FT}_{\overline{\psi}}(D\mathcal{H}).$$

In characteristic 2, where ψ takes values ± 1, we have $\overline{\psi} = \psi$. Therefore $\mathcal{F}(q, f)$ is self-dual if and only if $\mathcal{L}_{\psi_2([x^{t(q)},f(x)])}$ is self-dual. Its dual is $\mathcal{L}_{\psi_2(-[x^{t(q)},f(x)])}$. We have the Witt vector addition law $[x, y] = [x, 0] + [0, y]$, and, for Witt vectors over $\mathbb{F}_2$-algebras, $-[x, y] = [x, y + x^2]$. So the dual of $\mathcal{L}_{\psi_2([x^{t(q)},f(x)])}$ is $\mathcal{L}_{\psi_2([x^{t(q)},f(x)+(x^{t(q)})^2])}$, and the asserted isomorphism is

$$\mathcal{L}_{\psi_2([x^{t(q)},0])} \otimes \mathcal{L}_{\psi(f(x))} \cong \mathcal{L}_{\psi_2([x^{t(q)},0])} \otimes \mathcal{L}_{\psi(f(x)+(x^{t(q)})^2)}.$$

This holds if and only if there is an isomorphism

$$\mathcal{L}_{\psi(f(x))} \cong \mathcal{L}_{\psi(f(x)+(x^{t(q)})^2)},$$

or equivalently if $\mathcal{L}_{\psi((x^{t(q)})^2)}$ is geometrically trivial. By the Artin-Schreier reduction we have $\mathcal{L}_{\psi((x^{t(q)})^2)} \cong \mathcal{L}_{\psi(x^{t(q)})}$. The latter sheaf is not geometrically trivial, because $x^{t(q)}$ is a polynomial of odd degree $t(q)$ and so the sheaf has $\mathsf{Swan}_\infty(\mathcal{L}_{\psi(x^{t(q)})}) = t(q) \neq 0$. □

Corollary 5.8. *Suppose that the sheaf $\mathcal{F}(q, f)$ introduced in* (4.1.1) *is Lie-irreducible. Then it is not Lie-self-dual.*

Proof. Combine Theorem 5.6 and Theorem 5.7. □

Theorem 5.9. *The sheaf $\mathcal{F}(q, f)$ introduced in* (4.1.1) *is tensor indecomposable.*

Proof. We will show that $\mathcal{F}(q, f)$ is tensor indecomposable as a representation of $\pi_1 := \pi_1(\mathbb{A}^1/\overline{\mathbb{F}_p})$. Because π_1 has cohomological dimension ≤ 1 (this is true for the π_1 of any smooth, connected affine curve over an algebraically closed field), the argument of [KRLT1, Corollary 10.4] shows that if $\mathcal{F}(q, f)$ is tensor decomposable, then it is linearly tensor decomposable, i.e. we have an isomorphism of local systems on $\mathbb{A}^1/\overline{\mathbb{F}_p}$,

$$\mathcal{F}(q, f) \cong \mathcal{A} \otimes \mathcal{B},$$

with both $\mathrm{rank}(\mathcal{A}), \mathrm{rank}(\mathcal{B}) \geq 2$. To fix ideas, suppose $\mathrm{rank}(\mathcal{A}) \leq \mathrm{rank}(\mathcal{B})$. Then

$$\mathrm{End}(\mathcal{F}(q, f)) = \mathrm{End}(\mathcal{A}) \otimes \mathrm{End}(\mathcal{B}) = (\mathbb{1} + \mathrm{End}^0(\mathcal{A})) \otimes (\mathbb{1} + \mathrm{End}^0(\mathcal{B})) \text{ contains } \mathbb{1} + \mathrm{End}^0(\mathcal{A}).$$

Thus $\mathrm{End}^0(\mathcal{F}(q, f))$ contains $\mathrm{End}^0(\mathcal{A})$ as a direct factor. Now $\mathrm{End}^0(\mathcal{A})$ has rank less than

$$(\mathrm{rank}(\mathcal{A}))^2 \leq \mathrm{rank}(\mathcal{A})\mathrm{rank}(\mathcal{B}) = \mathrm{rank}(\mathcal{F}(q, f)).$$

So by Lemma 5.1, $\mathrm{End}^0(\mathcal{F}(q, f))$ contains some $\mathcal{L}_{\psi(ax)}$ with $a \neq 0$ ($a \neq 0$ because $\mathrm{End}^0(\mathcal{F}(q, f))$ only contains $\mathbb{1}$ once, by irreducibility of $\mathcal{F}$). The proof of Theorem 5.5 shows this is impossible. □

Lemma 5.10. *For every integer $n \geq 2$, the integer $2^n - 1$ is never a perfect power x^m with $x \in \mathbb{Z}$ and $m \geq 2$.*

Proof. We argue by contradiction. If $2^n - 1 = x^m$, then x is odd and $x^m = 2^n - 1 \equiv 3 \pmod 4$. Thus m is odd, and hence $2^n = x^m + 1$ is divisible by $x+1$. The quotient $\frac{x^m+1}{x+1} > 1$ is the alternating sum of m powers of the odd integer x, so is itself odd. Thus $\frac{x^m+1}{x+1}$ is an odd divisor of 2^n, the desired contradiction. □

Corollary 5.11. *For $n \geq 1$, no lisse sheaf of rank $2^n(2^{2n+1}-1)$ can be tensor induced. In particular, $\mathcal{F}(q, f)$ is not tensor induced.*

Theorem 5.12. *The local systems $\mathcal{F}(q, f)$ on $\mathbb{A}^1/\overline{\mathbb{F}_2}$ introduced in* (4.1.1) *all satisfy the condition* (**S**+) *of* [KT1, Definition 1.2].

Proof. First, by [Such, Proposition 7.4] the underlying representation V of G_{geom} of $\mathcal{F}(q, f)$ is irreducible. That $\mathcal{F}(q, f)$ is primitive, tensor indecomposable, and not tensor induced is the content of Theorem 5.5, Theorem 5.9 and Corollary 5.11. That $\det(\mathcal{F}(q, f))$ has finite order results from the fact that $\mathcal{F}(q, f)$ began life over a finite subfield of $\overline{\mathbb{F}_p}$ (in fact any subfield containing the coefficients of f). □

Theorem 5.13. *For the local system $\mathcal{F}(q, f)$ on $\mathbb{A}^1/\overline{\mathbb{F}_2}$ introduced in* (4.1.1), *every irreducible constituent of* $\text{End}^0(\mathcal{F}(q, f))$ *has dimension* $\geq \text{rank}(\mathcal{F}(q, f))$. *In particular, if $G_{\text{geom},\mathcal{F}(q,f)}$ is not finite, then $G^\circ_{\text{geom},\mathcal{F}(q,f)}$ is a simple algebraic group of dimension* $\geq \text{rank}(\mathcal{F}(q, f))$.

Proof. By Lemma 5.1, any irreducible constituent of dimension $< D := \text{rank}(\mathcal{F}(q, f))$ is a single $\mathcal{L}_{\psi(ax)}$, while Theorem 5.5 shows that $\text{End}^0(\mathcal{F}(q, f))$ contains no $\mathcal{L}_{\psi(ax)}$. Because $\mathcal{F}(q, f)$ satisfies condition (**S**+) by Theorem 5.12, if $G_{\text{geom},\mathcal{F}(q,f))}$ is not finite, then its identity component $G^\circ_{\text{geom},\mathcal{F}(q,f))}$ is a simple algebraic group. In that case, $\text{Lie}(G^\circ_{\text{geom},\mathcal{F}(q,f))})$ is an irreducible constituent of $\text{End}^0(\mathcal{F}(q, f))$, so has dimension $\geq D$. □

Theorem 5.14. *Consider the sheaf $\mathcal{F}(q, f)$ in* (4.1.1) *subject to the condition* (4.1.3). *Then, for each $r|t(q)$, the descent $\mathcal{G}(q, f, r)$ satisfies the condition* (**S**+) *of* [KT1, Definition 1.2].

Proof. Because $G_{\text{geom},\mathcal{F}(q,f)}$ is a subgroup of $G_{\text{geom},\mathcal{G}(q,f,r)}$ of finite index, the fact that $\mathcal{F}(q, f)$ satisfies condition (**S**+), see Theorem 5.12, implies that $\mathcal{G}(q, f, r)$ does as well. [Condition (**S**+) holds for (G, V) if it holds for (H, V) with H a subgroup of G of finite index.] □

We also record the following

Theorem 5.15. *Under the condition* (4.1.3), *if the sheaf $\mathcal{F}(q, f)$ in* (4.1.1) *is Lie-irreducible, then it is not Lie-self-dual.*

Proof. This is just a restatement of Corollary 5.8, under the more restrictive hypotheses of (4.1.3). Given Theorem 5.7, it suffices to show that if $\mathcal{F}(q, f)$ is Lie-irreducible and Lie-self-dual, then it is self-dual.

However, there is a simpler proof of this last fact, using the descent $\mathcal{G}(q, f) := \mathcal{G}(q, f, t(q))$ in Theorem 5.14. Exactly as in the proof of Theorem 5.6, we find an isomorphism

$$\mathcal{G}(q, f)^\vee \cong \mathcal{G}(q, f) \otimes \mathcal{L}$$

for some lisse $\mathcal{L}$ on $\mathbb{G}_m$ of rank one. Because $\mathcal{G}(q, f)^\vee$and $\mathcal{G}(q, f)$ are both tame at 0 and with all ∞-slopes < 1, $\mathcal{L}$ is tame on $\mathbb{G}_m$, hence a Kummer sheaf $\mathcal{L}_\chi$. Because $\mathcal{G}(q, f)^\vee$and $\mathcal{G}(q, f)$ both have $I(0)$ representations which are sums of characters of order dividing $t(q)$, χ is a ratio of characters of order dividing $t(q)$, so χ has order dividing $t(q)$. Pulling back this isomorphism by $t(q)^{\text{th}}$ power, we get an isomorphism $\mathcal{F}(q, f)^\vee \cong \mathcal{F}(q, f)$. □

6. A local system for the Suzuki group ${}^2B_2(8)$

Now we can prove the first main result of the paper, which establishes [Ka5, Conjecture 2.2] in the case $q = 8$:

Theorem 6.1. *Let $q = 8$. Both the local systems $\mathcal{F}_q$ and $\mathcal{G}_q$ have geometric monodromy group $G_{\mathrm{geom}} \cong {}^2B_2(8)$ in one of its irreducible representation of degree 14. Over $\mathbb{F}_2$, the local systems $\mathcal{F}_q$ and $\mathcal{G}_q$ have arithmetic monodromy group $G_{\mathrm{arith}} \cong \mathrm{Aut}({}^2B_2(8))$.*

Proof. (a) Let G, respectively H, denote the geometric monodromy group of $\mathcal{F}_q$, respectively of $\mathcal{G}_q$. Similarly, let G_{arith}, respectively H_{arith}, denote the arithmetic monodromy group of $\mathcal{F}_q$, respectively of $\mathcal{G}_q$, over $\mathbb{F}_2$. We will use the fact that $f := \mathrm{Frob}_{1,\mathbb{F}_2}$ has order 15 and trivial determinant. Indeed, a Magma calculation shows that

$$\mathrm{Trace}(\mathrm{Frob}_{1,\mathbb{F}_{2^{15}}}|\mathcal{G}_q) = \mathrm{Trace}(\mathrm{Frob}_{1,\mathbb{F}_{2^{15}}}|\mathcal{F}_q) = 14.$$

By Theorem 2.2, $\mathrm{Frob}_{1,\mathbb{F}_{2^{15}}}|\mathcal{G}_q$ is semisimple, hence (being of weight zero in a 14-dimensional representation) is the identity. Therefore $\det(\mathrm{Frob}_{1,\mathbb{F}_{2^{15}}}|\mathcal{G}_q))$ is a root of unity of order dividing both 4 (by Theorem 2.1) and 15, so this determinant is trivial. But $H_{\mathrm{arith}} = \langle f, H\rangle$, and H has trivial determinant (by Theorem 2.1), and hence H_{arith} also has trivial determinant. As $G \lhd H$ and $G_{\mathrm{arith}} \le H_{\mathrm{arith}}$ are subgroups, both G and G_{arith} have trivial determinants.

Recall that G is normal in H of index dividing $t(q) = 5$. By Theorem 5.12, H satisfies $(\mathbf{S}+)$. Since the rank of the sheaves is 14, not a prime power, by [KT1, Lemma 1.1] this implies that either the identity component H° of H is a simple algebraic group that acts irreducibly on the underlying representation V of H, or H is a finite almost quasisimple group with $L := H^{(\infty)}$ also acting irreducibly on V.

(b) Consider the former case. Note that if H° is classical of rank r, then either it is of type A and $r \le 13$, or $r \le 7$ by [KlL, Proposition 5.4.11]. Using the tables of [Lu], we see that H° is of type SL_2, SL_{14}, Sp_4, Sp_6, Sp_{14}, SO_{14}, or G_2. Since $[H : G] < \infty$, $G^\circ = H^\circ$.

Suppose first that $H^\circ = \mathrm{SL}_{14}(\mathbb{C})$. In this case, V is just the natural module for H°, hence $M_{2,2}(V)$ takes the smallest possible value 2 for all H°, H, G°, and G. But this contradicts Corollary 1.2.

Next suppose that $G^\circ = H^\circ$ is of type SL_2, Sp_4, Sp_6, Sp_{14}, SO_{14}, or G_2. In all these cases, the G°-module V is self-dual, and this contradicts Corollary 5.8.

(c) We have shown that H is finite, and we are in the almost quasisimple case. In this case, H_{arith} is also finite, and $H^{(\infty)}_{\mathrm{arith}} = H^{(\infty)} = G^{(\infty)}_{\mathrm{arith}} = G^{(\infty)} = L$. Let φ denote the character of H_{arith} in the underlying representation V. Then the formula for the trace function of $\mathcal{G}_q$ and the existence of an element with trace $2\zeta_4$ show that

$$\mathbb{Q}(\varphi) = \mathbb{Q}(\zeta_4). \tag{6.1.1}$$

Since any element z of $\mathbf{C}_{H_{\mathrm{arith}}}(L) = \mathbf{Z}(H_{\mathrm{arith}})$ acts as a root of unity γ on V, this implies that $\gamma^4 = 1$. Since H_{arith} has trivial determinant, $\gamma^{14} = 1$ and thus $\gamma = \pm 1$. It follows that

$$|\mathbf{C}_{H_{\mathrm{arith}}}(L)| = |\mathbf{Z}(H_{\mathrm{arith}})| \le 2. \tag{6.1.2}$$

Now, using (6.1.1) and the fact that L acts irreducibly on $V = \mathbb{C}^{14}$, the classification results of [HM] show that $L = \mathrm{PSL}_2(13)$, $\mathrm{SL}_2(13)$, A_7, A_8, $\mathrm{SU}_3(3)$, $G_2(3)$, $2 \cdot J_2$, A_{15}, or ${}^2B_2(8)$.

In all but the last case, $\varphi|_L$ is real-valued; furthermore, $|\mathrm{Out}(L)| \le 2$. As shown in the proof of Theorem 4.5, G has no subgroups of index 2, so G can induce only inner automorphisms of L. But $G_{\mathrm{arith}} = \langle G, f\rangle$, implying $G_{\mathrm{arith}}/G \hookrightarrow C_{15}$; so the same conclusion holds for G_{arith}, and hence $G_{\mathrm{arith}} = \mathbf{C}_{G_{\mathrm{arith}}}(L)L = \mathbf{Z}(G_{\mathrm{arith}})L$, with $|\mathbf{Z}(G_{\mathrm{arith}}| \le 2$ by (6.1.2). On the other hand, as we saw in the computation for the proof of Corollary 1.2, some $g \in G_{\mathrm{arith}}$ has trace $2\zeta_4$ on V. Write $g = zh$ with $z \in \mathbf{Z}(G_{\mathrm{arith}})$ and $h \in L$. It follows that $2\zeta_4 = \varphi(g) = \pm\varphi(h)$, a contradiction since $\varphi(h) \in \mathbb{R}$.

We have therefore shown that $L = {}^2B_2(8)$. As $|\mathrm{Out}(L)| = 3$, (6.1.2) implies that $|H/L|$ divides 6. On the other hand, H is the normal closure of the image of order 5 of $I(0)$, so we conclude that $H = L$. Since $L \lhd G \lhd H$, we also get $G = L$.

Recalling again that $G_{\mathrm{arith}}/G \hookrightarrow C_{15}$, we now see from (6.1.2) that $\mathbf{Z}(G_{\mathrm{arith}}) = 1$ and thus $G_{\mathrm{arith}} \hookrightarrow \mathrm{Aut}(L) \cong L \rtimes C_3$. A MAGMA computation shows the existence of a Frobenius element with trace ζ_4, and this implies that $G_{\mathrm{arith}} > L$, whence $G_{\mathrm{arith}} = \mathrm{Aut}(L)$. Since H_{arith} is generated over H by $f = \mathrm{Frob}_{1,\mathbb{F}_2}$, an element of order 15, $\mathbf{Z}(H_{\mathrm{arith}}) = 1$ by (6.1.2). Thus $H_{\mathrm{arith}} \hookrightarrow \mathrm{Aut}(L)$, and so $H_{\mathrm{arith}} = \mathrm{Aut}(L)$ as $H_{\mathrm{arith}} \geq G_{\mathrm{arith}}$. □

7. Low-dimensional representations of classical groups

In this section, we will extend the classification results obtained in [KlL, Proposition 5.4.11] and [Lu, Theorem 5.1]. Even though the intended applications in the paper only need the complex case of these results, we establish them in the modular case, which is interesting in its own right.

Let $\mathbb{F}$ be an algebraically closed field of characteristic $p \geq 0$ and let G be a simple, simply connected, classical algebraic group of rank r over $\mathbb{F}$. Fixing a maximal torus in G, we consider the set of simple roots $\{\alpha_1, \ldots, \alpha_r\}$ and the corresponding set of fundamental weights $\{\varpi_1, \ldots, \varpi_r\}$ (in the ordering of [OV]). Then the set

$$\Lambda^+ = \left\{ \sum_{i=1}^{r} a_i \varpi_i \mid a_i \in \mathbb{Z}, a_i \geq 0 \right\}$$

of dominant weights admits the partial ordering $\succ$ where $\lambda \succ \mu$ precisely when $\lambda - \mu = \sum_{i=1}^{r} k_i \alpha_i$ for some non-negative integers k_i. As usual, W denotes the Weyl group. If $\lambda \in \Lambda^+$, let $L(\lambda)$ denote the irreducible $\mathbb{F}G$-module with highest weight λ.

We will rely on the following two results.

Theorem 7.1. [Pr] *Let G be a simple, simply connected algebraic group in characteristic $p > 0$. If the root system of G has different root lengths, then we assume that $p \neq 2$, and if G is of type G_2, then we also assume that $p \neq 3$. Let λ be a restricted dominant weight. Then the set of weights $\Pi(\lambda)$ of the irreducible G-module $L(\lambda)$ is the union of the W-orbits of dominant weights μ with $\lambda \succ \mu$.* □

Lemma 7.2. [H, Lemma 10.3B] *Let $\lambda = \sum_{i=1}^{r} a_i \varpi_i$ be a dominant weight. Then the stabilizer of λ in the Weyl group is the Young subgroup generated by the reflections ρ_i along the simple roots α_i for which $a_i = 0$.* □

Our first result treats groups of type A and includes a strengthening for SL_{22}:

Theorem 7.3. *Let $G = \mathrm{SL}_n(\mathbb{F})$ with $n = r+1 \geq 8$, and let $L(\lambda)$ be an irreducible $\mathbb{F}G$-representation, which is restricted if $p = \mathrm{Char}(\mathbb{F}) > 0$. Suppose that $\dim L(\lambda) \leq M$, where $M := \binom{n}{4}$ if $n \neq 22$ and $M := 8176$ if $n = 22$. Then $\lambda = 0$, $a\varpi_1$ or $a\varpi_r$ with $1 \leq a \leq 3$, $\varpi_1 + \varpi_r$, ϖ_2 or ϖ_{r-1}, ϖ_3 or ϖ_{r-2}, ϖ_4 or ϖ_{r-3}, $\varpi_1 + \varpi_2$ or $\varpi_{r-1} + \varpi_r$, $2\varpi_1 + \varpi_r$ or $\varpi_1 + 2\varpi_r$, and $\varpi_2 + \varpi_r$ or $\varpi_1 + \varpi_{r-1}$.*

Proof. Write the highest weight λ as $\sum_{i=1}^{r} a_i \varpi_i$ with $a_i \in \mathbb{Z}_{\geq 0}$.

(a) First suppose that there is some weight $\mu = \sum_{i=1}^{r} b_i \varpi_i \in \Lambda^+$ with $\lambda \succ \mu$ and $b_j \neq 0$ for some $s + 1 \leq j \leq r - s$, where

$$s := 3 \text{ if } n \neq 22 \text{ and } s := 4 \text{ if } n = 22.$$

By Theorem 7.1, $\Pi(\lambda)$ contains the W-orbit $\mathcal{O}(\mu)$ of μ. By Lemma 7.2,

$$\mathrm{Stab}_W(\mu) \leq \langle \rho_1, \ldots, \rho_{j-1}, \rho_{j+1}, \ldots, \rho_r \rangle = \mathsf{S}_j \times \mathsf{S}_{n-j}$$

(where $\rho_i = (i, i+1) \in W = \mathsf{S}_n$). Hence

$$\dim L(\lambda) \geq |\mathcal{O}(\mu)| \geq [\mathsf{S}_n : (\mathsf{S}_j \times \mathsf{S}_{n-j})] = \binom{n}{j} \geq \binom{n}{s+1} \geq M,$$

a contradiction if $n = 22$, or if $5 \leq j \leq r-4$. Suppose $j \in \{4, r-3\}$ and $n \neq 22$. Then $\dim L(\lambda) = |\mathcal{O}(\mu)| = \binom{n}{4}$, showing μ is the unique dominant weight of $L(\lambda)$, whence $\mu = \lambda$. This also forces $\mathrm{Stab}_W(\lambda) = \mathsf{S}_j \times \mathsf{S}_{n-j}$, and so $\lambda = a_j\varpi_j$. Now if $a \geq 2$, then $\lambda \succ \lambda - \alpha_j = \varpi_{j-1} + (a_j - 2)\varpi_j + \varpi_{j+1}$, and the latter is another dominant weight of $L(\lambda)$, a contradiction. So $\lambda = \varpi_4$ or ϖ_{r-3} in such a case.

We may therefore assume that

$$a_j = 0 \text{ for every } s+1 \leq j \leq r-s. \tag{7.3.1}$$

Next suppose that $\sum_{i=1}^{s} ia_i \geq s+1$. By [GLT, Lemma 2.6] (applied with $m = s$), there is some weight $\mu = \sum_{i=1}^{r} b_i\varpi_i \in \Lambda^+$ with $\lambda \succ \mu$ and $b_{s+1} > a_{s+1}$. This situation is already considered by the preceding analysis. Using the symmetry under the graph automorphism τ of G,

$$\sum_{i=1}^{s} ia_i \leq s, \ \sum_{i=1}^{s} ia_{r+1-i} \leq s. \tag{7.3.2}$$

(b) Suppose $a_4 > 0$ or $a_{r-3} > 0$. By symmetry, we may assume $a_4 > 0$. By (7.3.2) $n = 22$, $a_4 = 1$, and $a_1 = a_2 = a_3 = 0$. Now if $\lambda \neq \varpi_4$, then $a_j \geq 1$ for some $r-3 \leq j \leq r$ by (7.3.1). By Lemma 7.2,

$$\mathrm{Stab}_W(\lambda) \leq \langle \rho_1, \rho_2, \rho_3, \rho_5, \rho_6, \ldots, \rho_{j-1}, \rho_{j+1}, \ldots, \rho_r \rangle \cong \mathsf{S}_4 \times Y_1,$$

with Y_1 a proper Young subgroup of S_{n-4} and hence $|Y_1| \leq (n-5)!$. It follows that

$$\dim L(\lambda) \geq [W : \mathrm{Stab}_W(\lambda)] \geq (n-4)\binom{n}{4} > M,$$

a contradiction. Hence from now on we may assume that $a_4 = a_{r-3} = 0$.

(c) Suppose that $a_3 > 0$ or $a_{r-2} > 0$. By symmetry, we may assume $a_3 > 0$, and so $a_3 = 1$ by (7.3.2). Suppose $a_j \geq 1$ for some $r-3 \leq j \leq r$. By Lemma 7.2,

$$\mathrm{Stab}_W(\lambda) \leq \langle \rho_1, \rho_2, \rho_4, \rho_5, \ldots, \rho_{j-1}, \rho_{j+1}, \ldots, \rho_r \rangle \cong \mathsf{S}_3 \times Y_2, \tag{7.3.3}$$

with Y_2 a proper Young subgroup of S_{n-3} and hence $|Y_2| \leq (n-4)!$. It follows that

$$\dim L(\lambda) \geq [W : \mathrm{Stab}_W(\lambda)] \geq (n-3)\binom{n}{3} > M$$

(as $n \geq 8$), a contradiction. Now, if $n \neq 22$, then using (7.3.1) and (7.3.2) we see that $\lambda = \varpi_3$. If $n = 22$ but $\lambda \neq \varpi_3$, then $\lambda = \varpi_1 + \varpi_3$. In this case, $\lambda - (\alpha_1 + \alpha_2 + \alpha_3) = \varpi_4$ is also a weight of $L(\lambda)$ by Theorem 7.1, and since

$$\mathrm{Stab}_W(\varpi_1 + \varpi_3) = \langle \rho_2, \rho_4, \rho_5, \ldots, \rho_r \rangle \cong \mathsf{S}_2 \times \mathsf{S}_{n-3}, \ \mathrm{Stab}_W(\varpi_4) = \mathsf{S}_4 \times \mathsf{S}_{n-4}$$

by Lemma 7.2,

$$|\mathcal{O}(\varpi_1 + \varpi_3)| + |\mathcal{O}(\varpi_4)| = \binom{22}{3}/2 + \binom{22}{4} = 11935 > M, \tag{7.3.4}$$

which contradicts $\dim L(\lambda) < M$.

(d) We may now assume that $a_i = 0$ for $3 \leq i \leq r-2$. Suppose that $a_2 > 0$ or $a_{r-1} > 0$. By symmetry, we may assume $a_2 > 0$. If $a_2 \geq 2$, then by (7.3.2) $n = 22$, $(a_2, a_1) = (2, 0)$. Note that $\lambda \succ \lambda - \alpha_2 = \varpi_1 + \varpi_3 + a_{r-1}\varpi_{r-1} + a_r\varpi_r$. It follows from Theorem 7.1 that $\Pi(\lambda)$ contains

$\varpi_1 + \varpi_3 + a_{r-1}\varpi_{r-1} + a_r\varpi_r$ and $\varpi_4 + a_{r-1}\varpi_{r-1} + a_r\varpi_r$. The lengths of W-orbits of these two weights are at least 11395 by (7.3.4), and so $\dim L(\lambda) > M$.

If $a_2 = 1$ but $a_1 \geq 2$, then by (7.3.2) $n = 22$, $(a_2, a_1) = (1, 2)$. Note that

$$\lambda \succ \lambda - \alpha_1 = 2\varpi_2 + a_{r-1}\varpi_{r-1} + a_r\varpi_r.$$

The preceding arguments show that $\Pi(\lambda)$ contains the weights $\varpi_1 + \varpi_3 + a_{r-1}\varpi_{r-1} + a_r\varpi_r$ and $\varpi_4 + a_{r-1}\varpi_{r-1} + a_r\varpi_r$, and again $\dim L(\lambda) > M$.

Hence $a_2 = 1$ and $a_1 \leq 1$. If $a_r = a_{r-1} = 0$, then $\lambda = \varpi_2$ or $\varpi_1 + \varpi_2$. So assume that $a_r + a_{r-1} > 0$.

Suppose that $a_{r-1} > 0$. Then by Lemma 7.2

$$\mathrm{Stab}_W(\lambda) \leq \langle \rho_1, \rho_3, \rho_4, \ldots, \rho_{r-2}, \rho_r \rangle = \mathsf{S}_2 \times \mathsf{S}_{n-4} \times \mathsf{S}_2. \tag{7.3.5}$$

It follows that

$$\dim L(\lambda) \geq [W : \mathrm{Stab}_W(\lambda)] \geq \frac{n!}{(n-4)! \cdot (2!)^2} > M,$$

a contradiction. Hence $a_{r-1} = 0$.

Suppose next that $a_r \geq 2$. Then

$$\lambda \succ \nu_1 := \lambda - \alpha_r = \lambda - (2\varpi_r - \varpi_{r-1}) = a_1\varpi_1 + \varpi_2 + (a_{r-1} + 1)\varpi_{r-1} + (a_r - 2)\varpi_r.$$

Thus $\nu_1 \in \Pi(\lambda) \cap \Lambda^+$, and (7.3.5) applied to ν_1 shows that

$$\dim L(\lambda) \geq |\mathcal{O}(\nu_1)| \geq [\mathsf{S}_n : (\mathsf{S}_2 \times \mathsf{S}_{n-4} \times \mathsf{S}_2)] > M.$$

We may therefore assume that $a_r = 1$. If $a_1 = 0$ then $\lambda = \varpi_2 + \varpi_r$. Otherwise $\lambda = \varpi_1 + \varpi_2 + \varpi_r$, in which case $\lambda \succ \nu_2 := \lambda - (\alpha_1 + \alpha_2) = \lambda - (\varpi_1 + \varpi_2 - \varpi_3) = \varpi_3 + \varpi_r$. But in such a case, (7.3.3) applied to ν_2 shows that

$$\dim L(\lambda) \geq |\mathcal{O}(\nu_2)| \geq (n-3)\binom{n}{3} > M.$$

(e) We may now assume that $a_i = 0$ for $2 \leq i \leq r-1$, i.e. $\lambda = a\varpi_1 + b\varpi_r$ with $s \geq a \geq b \geq 0$ (by symmetry). Suppose $a \geq 4$, whence $n = 22$ and $a = 4$ by (7.3.2). Then $\lambda \succ \lambda - 2\alpha_1 = 2\varpi_2 + b\varpi_r$, and so $\dim L(\lambda) > M$ by the first paragraph of (d).

Suppose $a = 3$ but $b > 0$. Then $\lambda \succ \nu_3 := \lambda - (2\alpha_1 + \alpha_2) = \lambda - (3\varpi_1 - \varpi_3) = \varpi_3 + b\varpi_r$, and (7.3.3) applied to ν_3 shows that $\dim L(\lambda) \geq |\mathcal{O}(\nu_3)| > M$. Hence $\lambda = \varpi_3$.

Suppose $a = b = 2$, i.e. $\lambda = 2\varpi_1 + 2\varpi_r$. Then $\lambda \succ \nu_4 := \lambda - (\alpha_1 + \alpha_r) = \varpi_2 + \varpi_{r-1}$. In such a case,

$$\dim L(\lambda) \geq |\mathcal{O}(\nu_4)| \geq \frac{n!}{(n-4)! \cdot (2!)^2} > M,$$

by using (7.3.5) for ν_4. So $a + b \leq 3$, and thus $\lambda = 2\varpi_1 + \varpi_r$, $2\varpi_1$, $\varpi_1 + \varpi_r$, ϖ_1, or 0. □

To handle the other classical groups, we first consider a special case. Again, we use the weight labeling as in [OV].

Proposition 7.4. *Let G be a simply connected simple algebraic group over $\mathbb{F}$ of type B_r, C_r, or D_r, with $r \geq 7$. Then*

$$\dim L(\varpi_1 + \varpi_2) \geq \begin{cases} 4r(r^2-1)/3, & \text{if } p = 3, \\ 4r(r-1)(2r-1)/3, & \text{if } p \neq 3. \end{cases}$$

Proof. Note that $|\mathcal{O}(\varpi_3)| = 8\binom{r}{3}$ and $|\mathcal{O}(\varpi_1 + \varpi_2)| = 4r(r-1)$. Since $\lambda := \varpi_1 + \varpi_2$ is the highest weight of $L(\lambda)$, it suffices to show that $\mu := \varpi_3$ is a weight of $L(\lambda)$, with multiplicity $m_{L(\lambda)}(\mu) \geq 1$ if $p = 3$ and $m_{L(\lambda)}(\mu) \geq 2$ if $p \neq 3$. If $p = 3$, then $\lambda \succ \lambda - (\alpha_1 + \alpha_2) = \mu$, whence $\mu \in \Pi(\lambda)$ by Theorem 7.1, and we are done.

In what follows we may assume $p \neq 3$. We realize the roots and the weights of G using an orthonormal basis $(e_i \mid 1 \leq i \leq r)$ of $\mathbb{R}^r$ (with scalar product $(\cdot,\cdot)$); in particular, $\varpi_1 = e_1$, $\varpi_2 = e_1 + e_2$, $\varpi_3 = e_1 + e_2 + e_3$. Consider the simple (Weyl) module $V(\lambda)$ of the corresponding algebraic group over $\mathbb{C}$. Then $\nu \in \Lambda^+$ is a weight of $V(\lambda)$ precisely when $\lambda \succ \nu$. Writing ϖ_i in terms of simple roots (see [OV, Table 2]), it is straightforward to check that this is equivalent to

$$\nu \in \begin{cases} \{\lambda, \mu, \varpi_1\}, & \text{if } G = C_r \text{ or } D_r, \\ \{\lambda, \mu, \varpi_2, 2\varpi_1, 0\}, & \text{if } G = B_r. \end{cases} \tag{7.4.1}$$

Next we use Freudenthal's formula [H, p. 122] to find the multiplicity $m_{V(\lambda)}(\mu)$ of μ as a weight of $V(\lambda)$. Then we must find all multiples $l\alpha$ of positive roots α, with $l \in \mathbb{Z}_{\geq 1}$, such that $\mu + l\alpha$ is a weight of $V(\lambda)$, i.e. W-conjugate to one of the weights listed in (7.4.1). Again using [OV, Table 2], we can check that this happens precisely when $l = 1$ and $\alpha = e_1 - e_2$, $e_1 - e_3$, $e_2 - e_3$. In all these cases, $\mu + l\alpha$ is W-equivalent to λ, and we readily obtain $m_{V(\lambda)}(\mu) = 2$.

Suppose now that

$$m_{L(\lambda)}(\mu) \leq 1. \tag{7.4.2}$$

This can happen only when μ is a weight of some composition factor $L(\nu_0)$ of a reduction modulo p of $V(\lambda)$, where ν_0 is listed in (7.4.1). Note that if ν is such a weight and $\nu \neq \mu$, then $\nu \not\succ \mu$. It follows that $\nu_0 = \mu$, i.e. $L(\mu)$ is a composition factor of a reduction modulo p of $V(\lambda)$. By the linkage principle, see [Jan], this implies that $w \circ \lambda = \mu$ for some $w \in W_p$. Here, the affine Weyl group W_p is generated by the map $\rho_{\alpha,l} \circ \lambda = \rho_\alpha \circ \lambda + lp\alpha$, where α is a simple root, $l \in \mathbb{Z}$ and ρ_α denotes the reflection corresponding to α; furthermore, $\rho_\alpha \circ \lambda = \rho_\alpha(\lambda + \delta) - \delta$, where $\delta := \sum_{i=1}^r \varpi_i$.

Write $|v|^2$ instead of (v, v) for $v \in \mathbb{R}^r$. Then, for any root α and any $l \in \mathbb{Z}$

$$|\rho_{\alpha,l} \circ \lambda + \delta|^2 = |\lambda + \delta|^2 + l^2p^2|\alpha|^2 + 2lp(\rho_\alpha(\lambda + \delta), \alpha).$$

Observe that $|\alpha|^2 \in \mathbb{Z}$ and

$$\big(\rho_\alpha(\lambda + \delta), \alpha\big) = \left((\lambda + \delta) - \frac{2(\lambda + \delta, \alpha)}{(\alpha, \alpha)}, \alpha\right) = -(\lambda + \rho, \alpha) \in \mathbb{Z}.$$

It follows that $|\rho_{\alpha,l} \circ \lambda + \delta|^2 \equiv |\lambda + \delta|^2 \pmod{\gcd(2, p)}$. Thus we have shown

$$\text{If two weights } \lambda,\ \mu \text{ are linked, then } |\lambda + \delta|^2 \equiv |\mu + \delta|^2 \pmod{\gcd(2, p)p}. \tag{7.4.3}$$

(Note that a slightly weaker result than (7.4.3), namely only modulo p, was obtained in [T, Lemma 2.1].) In our case, $|\lambda + \delta|^2 - |\mu + \delta|^2 = 6$. Applying (7.4.3), we conclude that (7.4.2) can happen only when $p = 3$. □

Theorem 7.5. *Let G be a simply connected simple algebraic group over $\mathbb{F}$ of type B_r, C_r, or D_r, with $r \geq 12$. Let $L(\lambda)$ be an irreducible $\mathbb{F}G$-representation, which is restricted if $p := \mathrm{Char}(\mathbb{F}) > 0$. Suppose that $\dim L(\lambda) \leq M$, where $M := 2(r+1)^3$ if $r \geq 14$, and $M := r^3$ if $r = 12, 13$. Then $\lambda = a\varpi_1$ with $0 \leq a \leq 3$, ϖ_2, ϖ_3, or $\varpi_1 + \varpi_2$. Moreover, if $\lambda = \varpi_1 + \varpi_2$ and $r \geq 16$, then $p = 3$.*

Proof. Write the highest weight λ as $\sum_{i=1}^r a_i\varpi_i$ with $a_i \in \mathbb{Z}_{\geq 0}$ (note that $L(\varpi_1)$ is the natural module for G).

(a) First suppose that $a_i > 0$ for some $r - 2 \leq i \leq r$. In this case, by Lemma 7.2, the length of the W-orbit $\mathcal{O}(\lambda)$ of λ is at least $[W : \mathrm{Stab}_W(\lambda)] \geq 2^{r-1} > M$.

Next suppose that $a_i > 0$ for some $4 \leq i \leq r - 3$. In this case, if G is of type X_r so that $W = W(X_r)$, then $\mathrm{Stab}_W(\lambda)$ is contained in $W(A_{i-1}) \times W(X_{r-i})$ by Lemma 7.2, hence

$$\dim L(\lambda) \geq |\mathcal{O}(\lambda)| \geq 2^i\binom{r}{i} \geq \min\big(2^4\binom{r}{4}, 2^{r-3}\binom{r}{3}\big) > 2(r+1)^3,$$

since $r \geq 9$.

Applying this argument to $\mu = \sum_{i=1}^{r} b_i \varpi_i \in \Pi(\lambda) \cap \Lambda^+$, we deduce that

$$b_i = 0 \text{ for } 4 \leq i \leq r. \tag{7.5.1}$$

(b) Suppose $a_3 > 0$. If $a_1 > 0$ or $a_2 > 0$, then $\mathrm{Stab}_W(\lambda) \leq W(A_1) \times W(X_{r-3})$, whence

$$|\mathcal{O}(\lambda)| \geq 4r(r-1)(r-2) > 2(r+1)^3 \tag{7.5.2}$$

(since $r \geq 9$), contradicting the bound on $\dim L(\lambda)$. So $\lambda = a_3\varpi_3$. Now, if $a_3 \geq 2$ (and so $p \neq 2$ as λ is restricted), then by Theorem 7.1

$$\lambda \succ \lambda - \alpha_3 = \varpi_2 + \varpi_4 \in \Pi(\lambda) \cap \Lambda^+,$$

violating (7.5.1). Hence $\lambda = \varpi_3$ in this case.

We have shown that $a_3 = 0$. Suppose $a_2 > 0$. Now, if $a_2 \geq 2$ (so again $p \neq 2$), then

$$\lambda \succ \lambda - \alpha_2 = (a_1+1)\varpi_1 + (a_2-2)\varpi_2 + \varpi_3 \in \Pi(\lambda),$$

leading to a contradiction by applying (7.5.2) to $\lambda - \alpha_2$. If $a_2 = 1$ but $a_1 \geq 2$, then $p \neq 2$ and

$$\lambda \succ \lambda - (\alpha_1 + \alpha_2) = (a_1-1)\varpi_1 + \varpi_3 \in \Pi(\lambda),$$

again yielding a contradiction by applying (7.5.2) to $\lambda - \alpha_1 - \alpha_2$. Hence $\lambda \in \{\varpi_2, \varpi_1 + \varpi_2\}$ in this case.

We are left with the case $\lambda = a\varpi_1$. If $a \geq 4$, then again $p \neq 2$ and

$$\lambda \succ \lambda - (2\alpha_1 + \alpha_2) = (a_1-3)\varpi_1 + \varpi_3 \in \Pi(\lambda),$$

leading to a contradiction by applying (7.5.2) to $\lambda - 2\alpha_1 - \alpha_2$. So $0 \leq a \leq 3$ as stated.

(c) We make some more comments about the cases $\lambda \in \{3\varpi_1, \varpi_3, \varpi_1 + \varpi_2\}$. Note that

$$3\varpi_1 - \alpha_1 = \varpi_1 + \varpi_2, \ (\varpi_1 + \varpi_2) - (\alpha_1 + \alpha_2) = \varpi_3.$$

So, assuming $p \neq 2$ when $\lambda = \varpi_1 + \varpi_2$, we may assume $\varpi_3 \in \Pi(\lambda)$ in all these three cases. It now follows from Lemma 7.2 that in these cases

$$\dim L(\lambda) \geq |\mathcal{O}(\varpi_3)| = 4r(r-1)(r-2)/3 > r^3.$$

Proposition 7.4 shows that if $p = 2$, then $\dim L(\varpi_1 + \varpi_2) > 8\binom{r}{3} > r^3$ (as $r \geq 12$), and if $r \geq 16$ and $p \neq 3$, then $\dim L(\varpi_1 + \varpi_2) > 4r(r-1)(2r-1)/3 > 2(r+1)^3$. Thus,

$$\text{If } r \geq 12 \text{ and } \dim L(\lambda) \leq r^3, \text{ then } \lambda \in \{0, \varpi_1, 2\varpi_1, \varpi_2\}. \tag{7.5.3}$$

This statement (7.5.3) was recorded in [Lu, Theorem 5.1], but we note that the treatment of the weights $a_1\varpi_1 + a_2\varpi_2$ therein is incorrect. Also note that $\dim L(\varpi_1 + \varpi_2)$ may be smaller than $2(r+1)^3$ when $p = 3$, see [Lu] for examples. □

8. A dichotomy for monodromy groups

We will need some preliminary facts:

Lemma 8.1. *Let $n \in \mathbb{Z}_{\geq 1}$ and let $D := 2^n(2^{2n+1} - 1)$. Then none of the following equations*

(i) $D = x^2 - 1$,
(ii) $D = x(x-1)/2$,
(iii) $D = x(x-1)/2 - 1$ *and* $n \geq 2$,

has a solution in the positive integers.

Proof. (i) Suppose $x^2-1=D$ for some $x\in\mathbb{Z}_{\geq 1}$. Checking the cases $1\leq n\leq 7$ directly, we may assume $n\geq 8$. Now $x>1$ is odd, and $\gcd(x-1,x+1)=2$, but $2^n|(x^2-1)$. It follows that there is some $\epsilon=\pm 1$ such that $2^{n-1}|(x-\epsilon)$. Write $x-\epsilon=2^{n-1}y$ for some $y\in\mathbb{Z}_{\geq 1}$. Then

$$2^{3n+1}-2^n=D=x^2-1=(2^{n-1}y+\epsilon)^2-1=2^{2n-2}y^2+2^n\epsilon y,$$

and so $\epsilon y+1=2^{n-2}(2^{n+3}-y^2)$. This implies $y>1$, and $y+\epsilon$ is divisible by 2^{n-2}. Hence $y+\epsilon=2^{n-2}z$ for some $z\in\mathbb{Z}_{\geq 1}$. In this case, $y\geq 2^{n-2}-1$, $x\geq 2^{2n-3}-2^{n-1}-1$, and so $x^2-1>2^{4n-7}\geq 2^{3n+1}>D$ (as $n\geq 8$), a contradiction.

(ii) Suppose $x(x-1)/2=D$ for some $x\in\mathbb{Z}_{\geq 1}$. Then $\gcd(x-1,x)=1$, but $2^{n+1}|x(x-1)$. It follows that there is some $\epsilon\in\{0,1\}$ such that $2^{n+1}|(x-\epsilon)$. Write $x-\epsilon=2^{n+1}y$ for some $y\in\mathbb{Z}_{\geq 1}$. If $\epsilon=0$, then

$$2^{3n+2}-2^{n+1}=2D=x(x-1)=2^{2n+2}y^2-2^{n+1}y,$$

and so $y-1=2^{n+1}(y^2-2^n)$. This implies $y>1$, and $y-1$ is divisible by 2^{n+1}. Hence $y-1\geq 2^{n+1}$, $x>2^{2n+2}$, and so $x(x-1)>2^{4n+4}>2^{3n+1}>D$, a contradiction. If $\epsilon=1$, then

$$2^{3n+2}-2^{n+1}=2D=x(x-1)=2^{2n+2}y^2+2^{n+1}y,$$

and so $y+1=2^{n+1}(2^n-y^2)$. This implies $1\leq y<2^{n/2}$, and $y+1$ is divisible by 2^{n+1}, which is impossible.

(iii) Suppose $n\geq 2$ and $D=x(x-1)/2-1=(x+1)(x-2)/2$ for some $x\in\mathbb{Z}_{\geq 1}$. Then $\gcd(x+1,x-2)|3$, but $2^{n+1}|(x+1)(x-2)$. It follows that there is some $\epsilon\in\{-1,2\}$ such that $2^{n+1}|(x-\epsilon)$. Write $x-\epsilon=2^{n+1}y$ for some $y\in\mathbb{Z}_{\geq 1}$. If $\epsilon=-1$, then

$$2^{3n+2}-2^{n+1}=2D=(x+1)(x-2)=2^{2n+2}y^2-3\cdot 2^{n+1}y,$$

and so $3y-1=2^{n+1}(y^2-2^n)$. This implies that $3y-1\geq 2$ is divisible by 2^{n+1}. Hence $y\geq(2^{n+1}+1)/3>2^{n-1}$, $x+1>2^{2n}$, and so $(x+1)(x-2)>2^{2n}(2^{2n}-3)>2^{3n+1}>D$ (as $n\geq 2$), a contradiction. If $\epsilon=2$, then

$$2^{3n+2}-2^{n+1}=2D=(x+1)(x-2)=2^{2n+2}y^2+3\cdot 2^{n+1}y,$$

and so $3y+1=2^{n+1}(2^n-y^2)$. This implies $1\leq y<2^{n/2}\leq 2^{n-1}$, and $3y+1$ is divisible by 2^{n+1}, which is impossible when $n\geq 2$. □

Note that if $(n,D)=(1,14)$, then $D=\binom{6}{2}-1=\binom{6}{3}-6=(3^3+1)/2$.

Theorem 8.2. *Suppose the sheaf $\mathcal{F}(q,f)$ in (4.1.1), of rank $D=2^n(2^{2n+1}-1)$, has infinite geometric monodromy group $G=G_{\mathrm{geom}}$. Then $G^\circ=\mathrm{SL}_D$. Under the more restrictive condition (4.1.3) $G=\mathrm{SL}_D$; moreover, the sheaf $\mathcal{G}(q,f,t(q))$ has geometric monodromy group equal to G.*

Proof. By Theorem 5.12, G satisfies (**S**+). Thus $G^\circ\leq\mathrm{SL}_D$, and $\mathbf{Z}(G)$ is finite, but G° is infinite. It follows from [KT1, Lemma 1.4] that G° is irreducible on the underlying representation V, i.e. $\mathcal{F}(q,f)$ is Lie-irreducible. By Theorem 5.13, G° is a simple algebraic group of dimension $\geq D$.

(a) Suppose $n\geq 3$, so that $D\geq 1016$. Then G° must be a classical group of rank say r, where $r(2r+1)\geq\dim G^\circ\geq D\geq 1016$, whence $r\geq 23$. Also, if G° is of type A_r, then

$$D\leq\dim G^\circ=r(r+2)<\binom{r+1}{4},\tag{8.2.1}$$

and if G° is of type B_r, C_r, or D_r, then

$$D\leq r(2r+1)<r^3.\tag{8.2.2}$$

In the case of A_r, we can apply Theorem 7.3 and, using the dimension formula for $L(\lambda)$ given in [OV, Table 5] and the bound (8.2.1), we see that the highest weight λ of the G°-module V is, up

to duality, $a\varpi_1$ with $a = 1, 2$, ϖ_2, or $\varpi_1 + \varpi_r$. If $\lambda = \varpi_1$, then $D = r + 1$, $G^\circ = \mathrm{SL}_D$, and hence $G = \mathrm{SL}_D$ as stated. In the other cases, $D = \binom{r+1}{2}$, $\binom{r}{2}$, or $(r+1)^2 - 1$; all are impossible by Lemma 8.1.

In the case of types B_r, C_r, and D_r, we can apply Theorem 7.5 (more precisely, (7.5.3)), and, using the dimension formula for $L(\lambda)$ given in [OV, Table 5] and the bound (8.2.2), we see that the highest weight λ of the G°-module V is $a\varpi_1$ with $a = 1, 2$, or ϖ_2. If $\lambda = \varpi_1$, then $G^\circ = \mathrm{Sp}(V)$ or $\mathrm{SO}(V)$, whence $\mathcal{F}(q, f)$ is Lie-self-dual, contrary to Corollary 5.8. In the other cases, $D = \binom{m}{2}$ or $\binom{m}{2} - 1$ for some integer $m \geq 2$, and this is impossible by Lemma 8.1.

(b) Suppose $n = 2$, so that $D = 124$. Then G° is of type A_r with $r \geq 11$, B_r, C_r, or D_r with $r \geq 8$, E_7, or E_8. Neither E_7 nor E_8 has irreducible representations of degree 124, see [Lu], so G° is classical of rank r. If G° is of type B_r, C_r, or D_r with $8 \leq r \leq 11$, then using [Lu] we check that G° has no irreducible representation of degree 124. So $r \geq 12$, and we apply Theorem 7.3, respectively (7.5.3), as above to conclude that $G = \mathrm{SL}_D$.

Finally, assume that $n = 1$, so that $D = 14$. The arguments in part (b) of the proof of Theorem 6.1 repeated verbatim show that either $G^\circ = \mathrm{SL}_D$, or $V|_{G^\circ}$ is self-dual. In the former case $G = \mathrm{SL}_D$ as in (a), and the latter case is ruled out by Corollary 5.8.

(c) Now assume (4.1.3). Then we can consider the descent $\mathcal{G}(q, f, t(q))$, for which the trace function takes values in $\mathbb{Q}(\zeta_4)$ and all slopes are less than 1. Since $p = 2$, Theorem 2.1(iii) implies that $\mathcal{G}(q, f, t(q))$ has trivial determinant, and thus $\mathcal{G}(q, f, t(q))$ has geometric monodromy group $H \leq \mathrm{SL}_D$. But $H \geq G$, so we conclude $H = G = \mathrm{SL}_D$. □

Theorem 8.3. *Suppose the sheaf $\mathcal{F}(q, f)$ in (4.1.3), of rank $D = 2^n(2^{2n+1} - 1)$, has finite geometric monodromy group $G = G_{\mathrm{geom}}$. Then $G = {}^2B_2(q)$ with $q = 2^{2n+1}$.*

Proof. (a) Let V denote the underlying representation. By Theorem 5.12, G satisfies (**S**+) on V. But the dimension $D = \dim(V) = q_0(q-1)$, with $q_0 := 2^n$, is not a prime power. Hence G is almost quasisimple by [KT1, Lemma 1.1]: $S \lhd G/\mathbf{Z}(G) \leq \mathrm{Aut}(S)$ for some finite, non-abelian simple group S. Then the quasisimple subgroup $L := G^{(\infty)}$ acts irreducibly on V by [KT1, Lemma 1.4].

The condition (4.1.3) allows us to consider the descent $\mathcal{G}(q, f, t(q))$ on $\mathbb{G}_m$, with geometric monodromy group H. Then $G \lhd H$ of finite index, whence H is finite and satisfies (**S**+), and $L = H^{(\infty)}$, as $H/G \hookrightarrow C_{t(q)}$. The representation of H on V has ∞-slopes $\sigma := (q_0 + 1)/D < 1$, and is not tame at ∞. Hence Theorem 2.5 applies to G and H. We collect some further facts about (G, V) and the character φ of H on V that we will use in the proof:

(i) $\mathbb{Q}(\varphi|_G) = \mathbb{Q}(\varphi) = \mathbb{Q}(i)$. Indeed, by Theorem 2.1(i), the arithmetic monodromy group H_{arith,k_0} of $\mathcal{G}(q, f, t(q))$ over k_0 has finite determinant. But it normalizes the finite irreducible subgroup H, so finite determinant implies that H_{arith,k_0} is finite. Now, by Chebotarev density, the finiteness of H_{arith,k_0} implies that all elements of it are Frobenii, and all Frobenii have traces in $\mathbb{Q}(i)$. But $G \leq H \leq H_{\mathrm{arith},k_0}$, so $\mathbb{Q}(\varphi|_G) \subseteq \mathbb{Q}(\varphi) \subseteq \mathbb{Q}(i)$. But $V|_G$ is not self-dual by Theorem 5.7, hence $\mathbb{Q}(\varphi|_G) = \mathbb{Q}(i) = \mathbb{Q}(\varphi)$. Since each element of $\mathbf{Z}(H)$ acts as a root of unity on V, and the only roots of unity in $\mathbb{Q}(i)$ are in μ_4, both $|\mathbf{Z}(G)|$ and $|\mathbf{Z}(H)|$ divide 4.

(ii) If $n \neq 2$, then G is perfect and hence $G = L$. Indeed, by [Abh, Proposition 6], $\pi_1(\mathbb{A}^1/\overline{\mathbb{F}_p})$ has no nontrivial finite p'-quotient. Since $\mathcal{F}(q, f)$ lives on $\mathbb{A}^1/\overline{\mathbb{F}_2}$, G has no nontrivial quotient of odd order. On the other hand, the proof of Theorem 4.5 shows that G has no quotient of order 2 when $n \neq 2$.

(iii) The image $J = QC$ of $I(\infty)$ has $Q = \mathbf{O}_2(J)$ and $C = \langle g_\infty \rangle$, where the central order $\bar{\mathsf{o}}(g_\infty)$ is divisible by $q - 1$. Indeed, since the ∞-slope of $\mathcal{F}(q, f)$ is $1 + 1/D$, this implies, by [Ka1, Proposition 1.14], that $I(\infty)$ acts irreducibly on V, of dimension $D = q_0(q-1)$. Since the

image J of $I(\infty)$ is cyclic of p'-order modulo the image Q of $P(\infty)$, it follows that g_∞ permutes the pairwise non-isomorphic $q-1$ simple Q-summands on V, each of dimension q_0, transitively.

(b) Consider the case $n \geq 3$, so that $D \geq 1016$, and $G = L$ by (ii).

(b1) First suppose that $S = \mathsf{A}_m$ for some $m \geq 3$. As $G/\mathbf{Z}(G) = \mathsf{A}_m \hookrightarrow \mathrm{GL}_{m-1}(\mathbb{C})$, by Theorem 2.5, $m - 1 \geq 1/\sigma$. Note that $\lceil 1/\sigma \rceil = q - 2q_0 + 1$, so $m \geq q - 2q_0 + 2 \geq 114$. It follows that $D = q_0(q-1) < (m^2 - 5m + 2)/2$. In this case, by [GT, Lemma 6.1] $m = D + 1$, $G = \mathsf{A}_{D+1}$, and $V = \mathbb{C}^D$ is the heart of the natural permutation module. But then V is self-dual, contrary to (i).

(b2) Next suppose that S is a sporadic simple group. By (iii), the maximum order $\mathsf{meo}(S)$ of elements in S is at least $q - 1 \geq 127$. On the other hand, $\mathsf{meo}(S) \leq 119$, as one can check using the [Atlas] (see also [KT1, Table 2]), a contradiction.

(b3) Consider the case S is a simple group of Lie type in characteristic $r \neq 2$. By Theorem 2.5, the degree e of every nontrivial projective representation over $\overline{\mathbb{F}_r}$ of S satisfies $e^2 - 1 \geq 1/\sigma$, in particular, $e \geq 11$. Similarly, the degree d of every faithful linear representation over $\overline{\mathbb{F}_r}$ of S satisfies $d \geq 1/\sigma$, in particular, $d \geq 114$. This rules out all classical groups of types A_m or ${}^2A_m$ with $m \leq 9$, B_m with $m \leq 56$, and C_m or D_m with $m \leq 7$ (as $\mathrm{PSp}_{2m}(r^a)$ and $\mathrm{P}\Omega^{\pm}_{2m}(r^a)$ have faithful representations of degree $m(2m-1)$ over $\overline{\mathbb{F}_r}$). This also rules out exceptional groups of types G_2, ${}^2G_2$, and ${}^3D_4$. For the remaining exceptional groups of type $F_4(s)$, $E_6(s)$, ${}^2E_6(s)$, $E_7(s)$, and $E_8(s)$, with $s = r^a$, by [KS, Table A7] we have the following upper bounds $s(s+1)(s^2+1)$, $s(s^6-1)/((s-1)\gcd(3,s-1))$, $(s+1)(s^2+1)(s^3-1)/\gcd(3,s+1)$, $(s+1)(s^2+1)(s^4+1)/2$, and $(s+1)(s^2+s+1)(s^5-1)$ for $\mathsf{meo}(S)$, respectively. On the other hand, $q_0(q-1) = D$ is at least the smallest degree $\mathfrak{d}(S)$ of nontrivial projective complex representations of S, which in turn is at least $s^6(s^2-1)$, $s^9(s^2-1)$, $s^9(s^2-1)$, $s^{15}(s^2-1)$, $s^{27}(s^2-1)$, respectively, see e.g. [TZ, Table I], and we arrive at a contradiction in all five cases, as $q - 1 \leq \mathsf{meo}(S)$ by (iii) and $D < \sqrt{q^3/2}$.

If $S = \mathrm{PSL}_m(s)$ or $\mathrm{PSU}_m(s)$ with $m \geq 11$, then $m^2 - 1 \geq 1/\sigma$, and so $m^2 \geq q - 2q_0 + 2$, by Theorem 2.5. Since $m \geq 11$, by [TZ, Theorem 1.1]

$$D \geq \frac{s^m - s}{s+1} \geq \frac{3^m - 3}{4} > m^3 \geq (q - 2q_0 + 2)^{3/2} > q_0(q-1),$$

a contradiction. For S of type BCD_m with $m \geq 7$, we have $\min(m(2m-1), 2m+1) \geq 1/\sigma$, and so $2m^2 \geq q - 2q_0 + 1$, by Theorem 2.5. Since $m \geq 7$, by [TZ, Theorem 1.1]

$$D \geq \frac{s^m - 1}{2} \geq \frac{3^m - 1}{2} > 3m^3 \geq (3/2^{3/2})(q - 2q_0 + 1)^{3/2} > q_0(q-1),$$

again a contradiction.

(b4) We may now assume that S is a simple group of Lie type in characteristic 2, defined over a field $\mathbb{F}_s$ with $s = 2^a$. Since $n \geq 3$, by Theorem 3.4, $t(q) = q - 2q_0 + 1$ admits a divisor $\ell = \mathrm{ppd}(2, 4(2n+1))$. Next, we use the fact that the image of $I(0)$ in H has order $q - 2q_0 + 1$, which implies that H has an element of prime order ℓ that normalizes $G = L$. But $\mathbf{C}_H(G) = \mathbf{Z}(H)$ has order dividing 4 by (i), so

$$\ell \text{ divides } |\mathrm{Aut}(L)|. \tag{8.3.1}$$

First suppose that $S = \mathrm{Sp}_{2m}(s)$ with $m \geq 2$ or $\mathrm{P}\Omega^{\pm}_{2m}(s)$ with $m \geq 3$. Then, (8.3.1) implies that $\ell \geq 4(2n+1) + 1 \geq 29$ divides $a|S|$. If moreover $\ell \nmid a$, then ℓ divides $\prod_{i=1}^{m}(s^{2i} - 1)$, which implies $2ma \geq 4(2n+1)$ by primitivity of ℓ. In either case,

$$s^m = 2^{ma} \geq 2^{2(2n+1)} = q^2 \geq 2^{14} \tag{8.3.2}$$

Now, applying [TZ, Theorem 1.1] for $m \geq 3$ we obtain

$$q^{3/2} > D \geq \mathfrak{d}(S) \geq \frac{(s^m-1)(s^{m-1}-1)}{s^2-1} > s^{2m-3}/2 \geq s^m/2 \geq q^2/2,$$

a contradiction. If $S = \mathrm{PSp}_4(s)$, then $s \geq q \geq 2^7$ by (8.3.2), and so

$$q^{3/2} > D \geq \mathfrak{d}(S) = s(s-1)^2/2 \geq q(q-1)^2/2 > q^2,$$

again a contradiction.

Next suppose that $S = \mathrm{PSL}_m(s)$ or $\mathrm{PSU}_m(s)$ with $m \geq 2$. The same arguments as above show that (8.3.2) still holds; in fact, $s^m \geq q^4$ for $S = \mathrm{PSL}_m(s)$. Assume that $S = \mathrm{PSL}_m(s)$ with $m \geq 2$; in particular, $s^{m-1} \geq s^{m/2} \geq q^2$. Then using [TZ, Theorem 1.1] we obtain that

$$q^{3/2} > D \geq \mathfrak{d}(S) \geq \frac{s^m - s}{s-1} > s^{m-1} \geq q^2,$$

a contradiction. Next, assume that $S = \mathrm{PSU}_m(s)$ with $m \geq 5$; in particular, $q^{3/2} \leq s^{3m/4} \leq s^{m-5/4}$. Then using [TZ, Theorem 1.1] we obtain that

$$\frac{q^{3/2}}{\sqrt{2}} > D \geq \mathfrak{d}(S) \geq \frac{s^m - s}{s+1} \geq \frac{2}{3}(s^{m-1}-1) > \frac{2^{5/4}}{3}(s^{m-5/4}-1) > \frac{2^{5/4}}{3}(q^{3/2}-1) > \frac{q^{3/2}}{\sqrt{2}},$$

again a contradiction. When $S = \mathrm{PSU}_4(s)$, $\ell | a$ or ℓ divides $(s+1)(s^2-1)(s^3+1)(s^4-1)$, so instead of (8.3.2) now $s^3 \geq q^2$. Again using [TZ, Theorem 1.1] we obtain

$$q^{3/2} > D \geq \mathfrak{d}(S) \geq \frac{s^4-1}{s+1} > s^3/2 \geq q^2/2,$$

a contradiction. Finally, if $S = \mathrm{PSU}_3(s)$, then $s^3 \geq q^2 \geq 2^{14}$ from (8.3.2). But every irreducible character of $\mathrm{SU}_3(s)$ of even degree has degree divisible by $s \geq q^{2/3}$, and hence cannot be equal to $D = q_0(q-1)$.

Let S be one of the exceptional groups of type $G_2(s)$ with $s > 2$, ${}^3D_4(s)$, ${}^2F_4(s)'$ with $s > 2$, $F_4(s)$ with $s > 2$, $E_6(s)$, ${}^2E_6(s)$, $E_7(s)$, and $E_8(s)$. That ℓ divides $|\mathrm{Aut}(S)|$ implies $q^4 \leq s^c$, where

$$c = 6,\ 12,\ 12,\ 12,\ 12,\ 18,\ 18,\ 30,$$

respectively. It follows that $D < q^{3/2} \leq s^{3c/8}$, with

$$3c/8 = 9/4,\ 9/2,\ 9/2,\ 9/2,\ 9/2,\ 27/4,\ 27/4,\ 45/4,$$

respectively. But this contradicts the lower bounds $D \geq \mathfrak{d}(S) \geq s(s^2-1)$, $s^3(s^2-1)$, $s^4(s-1)\sqrt{s/2}$, $s^6(s^2-1)$, $s^9(s^2-1)$, $s^9(s^2-1)$, $s^{15}(s^2-1)$, $s^{27}(s^2-1)$, respectively, see e.g. [TZ, Table I], and we arrive at a contradiction in all eight cases. The cases ${}^2F_4(2)'$ and $F_4(2)$ are ruled out because $|\mathrm{Aut}(S)|$ is not divisible by the prime $\ell \geq 29$.

The only remaining case is that $S = {}^2B_2(s)$. That ℓ divides $|\mathrm{Aut}(S)|$ implies $q^4 \leq s^4$, i.e. $q \leq s$. But $D = q_0(q-1)$ is the degree of some irreducible character of G, so $q = s$, i.e. $S = {}^2B_2(q)$. In this case also $G = L = {}^2B_2(q)$, as stated.

(c) Now we consider the case $n = 2$, i.e. $D = 124$.

(c1) As the quasisimple subgroup $L = G^{(\infty)}$ acts irreducibly on $V = \mathbb{C}^D$, by [HM] we have the following possibilities for S:

$$\mathrm{PSL}_2(125),\ \mathrm{SL}_3(5),\ \mathrm{SL}_5(2),\ G_2(5),\ \mathsf{A}_{125},\ \text{or } {}^2B_2(32).$$

Here, a generator g_0 of the image of $I(0)$ in H has order $t(q) = 25$ and normalizes G and L. Since $\mathbf{C}_H(L) = \mathbf{Z}(H) \leq C_4$ by (i), 25 divides $|\mathrm{Aut}(S)|$. This rules out the first three cases.

In the two cases $S = G_2(5)$ and A_{125}, $L = S$ and $V|_L$ is self-dual. Since $\mathbf{C}_H(L) \leq C_4$ and $|\mathrm{Out}(S)| \leq 2$, it follows that H/L is a 2-group. On the other hand, H has no quotient of order 2, as shown in part (i) of the proof of Theorem 4.5 (which also works for $n = 2$). Hence $H = L = G$, and so $\mathcal{F}(q, f)$ is self-dual. But this contradicts Theorem 5.7.

The only remaining case is $S = {}^2B_2(32)$, in which case $L = S$.

(c2) The rest of this paragraph applies to all $n \geq 1$, for which we know $L = S = {}^2B_2(q)$. Since $\mathrm{Out}(S) \cong C_{2n+1}$, but $G = \mathbf{O}^{2'}(G)$, we see that $G = \mathbf{Z}(G)S$, with $\mathbf{Z}(G) \leq C_4$. Recall that $H/G \hookrightarrow C_{t(q)}$ and $\mathbf{Z}(H) \leq C_4$. In particular, $\mathbf{Z}(H)G/G \cong \mathbf{Z}(H)/\mathbf{Z}(G)$ has order dividing both 4 and $t(q)$, whence $\mathbf{Z}(H) = \mathbf{Z}(G)$. Next, H/G acts trivially on $G/S \cong \mathbf{Z}(G)$, i.e. $G/S \leq \mathbf{Z}(H/S)$, and the quotient $(H/S)/(G/S) \cong H/G$ is cyclic. It follows that H/S is an abelian group. As mentioned above, H has no quotient of order 2, so $2 \nmid |H/S|$, whence $\mathbf{Z}(G) = 1$; in particular $G = S$ when $n = 2$. We have also shown that $\mathbf{C}_H(S) = \mathbf{Z}(H) = 1$, so

$$S \lhd H \leq \mathrm{Aut}(S) = S \rtimes C_{2n+1} \tag{8.3.3}$$

(d) Finally, we consider the case $n = 1$, i.e. $D = 14$. As the quasisimple group $G = L$ acts irreducibly on $V = \mathbb{C}^D$ and $\mathbb{Q}(\varphi) = \mathbb{Q}(i)$, by [HM] the only possibility is that $G = {}^2B_2(8)$. □

Now we are ready to prove the second main result of the paper:

Theorem 8.4. *For the geometric monodromy group $G = G_{\mathrm{geom}}$ of the sheaf $\mathcal{F}(q, f)$ in (4.1.3), of rank $D = 2^n(2^{2n+1} - 1)$, either $G = \mathrm{SL}_D$ or $G = {}^2B_2(q)$ with $q = 2^{2n+1}$. Furthermore, for any $r|t(q)$, the geometric monodromy group of the descent $\mathcal{G}(q, f, r)$ is also equal to G.*

Proof. Suppose G is infinite. Then the statements follow from Theorem 8.2.

From now on, assume that G is finite. Then $G = S = {}^2B_2(q)$ by Theorem 8.3. Since for any $r|t(q)$, the geometric monodromy group of $\mathcal{G}(q, f, r)$ contains G and is contained in the geometric monodromy group H of $\mathcal{F}(q, f, t(q))$, it suffices to show that $H = S$.

First, note that the ∞-slope of $\mathcal{G}(q, f, t(q))$ is $\sigma = (q_0 + 1)/D$ and $D + 1 = (q_0 + 1)t(q)$, so $\gcd(D, q_0 + 1) = 1$. It follows from [Ka1, Proposition 1.14] that $I(\infty)$ acts irreducibly on V, of dimension $D = q_0(q - 1)$. Since the image J of $I(\infty)$ is cyclic of p'-order modulo the image Q of $P(\infty)$, $Q = \mathbf{O}_2(J)$ and $J = \langle Q, g_\infty \rangle$, where the p'-element g_∞ transitively permutes the pairwise non-isomorphic $q - 1$ simple Q-summands on V, each of dimension q_0.

Since $q = 2^{2n+1}$, using [Zs] we can find a primitive prime divisor $\ell = \mathrm{ppd}(2, 2n + 1)$, and fix a power h of g_∞ that has order ℓ. Clearly, the prime ℓ is at least $2n + 3$, so it is coprime to $2n + 1 = |\mathrm{Out}(S)|$. On the other hand, $S \leq H \leq \mathrm{Aut}(S)$ by (8.3.3). Hence $h \in S$ and $Q < S$.

We can write $h = x^{(q-1)/\ell}$, where on the natural module $U = \mathbb{F}_q^4$ for $S = {}^2B_2(q) < \mathrm{Sp}(U)$, the spectrum of $x \in S$ consists of 4 eigenvalues ξ^{2^n}, ξ^{-2^n}, ξ^{1-2^n}, ξ^{2^n-1} where $\xi \in \overline{\mathbb{F}_2}^\times$ has order $q - 1$ see [Bur], [Suz]. We may write $\mathrm{Aut}(S) = \langle S, \theta \rangle$, where θ acts as the Galois automorphism $\lambda \mapsto \lambda^2$ of $\overline{\mathbb{F}_2}$. Suppose that for some $1 \leq a \leq 2n$ and for some $y \in S$, the element $y\theta^a$ centralizes h. Note that θ^a sends x to x^{2^a} and $h = x^{(q-1)/\ell}$ to $x^{2^a(q-1)/\ell}$. It follows that

$$x^{2^a(q-1)/\ell} = \theta^a h \theta^{-a} = y^{-1}(y\theta^a)h(y\theta^a)^{-1}y = y^{-1}hy$$

is S-conjugate to $h = x^{(q-1)/\ell}$. On the other hand, it is known [Bur] that if $b, c \in \mathbb{Z}$ then x^b and x^c are S-conjugate if and only if $c \equiv \pm b \pmod{(q-1)}$. It follows that ℓ divides $2^a \pm 1$; in particular, ℓ divides $2^{2a} - 1$. The primitivity of ℓ then implies that $2n + 1$ divides $2a$, a contradiction.

We have shown that $\mathbf{C}_{\mathrm{Aut}(S)}(h) \leq S$. As g_∞ centralizes h, it follows that $g_\infty \in S$. Hence $J = Q\langle g_\infty \rangle < S$. Now $S \lhd H$ and H is finite, so $H = S$ by Theorem 4.3. □

Theorems 6.1 and 8.4 imply the following.

Corollary 8.5. *The sheaves $\mathcal{F}_q$ and $\mathcal{G}_q$ in §1, of rank $D = 2^n(2^{2n+1}-1)$, have the same geometric monodromy group $G = G_{\rm geom}$. Furthermore, either $G = {}^2B_2(q)$ with $q = 2^{2n+1}$, or $n \geq 2$ and $G = {\rm SL}_D$.*

Remark 8.6. It is plausible that for each $q = 2^{2n+1} \geq 32$, we can find a polynomial $f_1 \in \mathbb{F}_2[x]$ of degree $2^n + 1$ such that the sheaf $\mathcal{F}(q, f)$ with $f(x) = f_1(x^{t(q)})$ as in (4.1.3) has infinite geometric monodromy group, which then is ${\rm SL}_D$ by Theorem 8.4. Indeed, a Magma calculation shows for each $2 \leq n \leq 25$ that ${\rm Frob}_{1,\mathbb{F}_{2^{k(n)}}}$ has non-integral trace on $\mathcal{F}(q, x^{(1+2^n)t(q)})$ for some choice of $k(n) \in \mathbb{Z}_{\geq 1}$. For instance, ${\rm Frob}_{1,\mathbb{F}_{2^{k(n)}}}$ has trace $(2i-7)/2$ for $(n, (k(n)) = (2, 7)$, $(5i+3)/2$ for $(n, k(n)) = (3, 5)$, $(7-3i)/4$ for $(n, k(n)) = (4, 7)$, and $5/2$ for $(n, k(n)) = (5, 7)$. In fact, for infinitely many integers $n \geq 2$, we offer in Theorem 9.18 a construction of a sheaf $\mathcal{F}(q, f)$ with $G_{\rm geom} = {\rm SL}_D$.

9. Arithmetic vs. geometric monodromy groups

9A. Glauberman and Dade correspondences. Our next results depend on the Glauberman correspondence. Recall that if A is a solvable finite group acting by automorphisms on another finite group S with $(|A|, |S|) = 1$, then there exists a canonical bijection $^* : {\rm Irr}_A(S) \to {\rm Irr}(C)$, where $C = \mathbf{C}_S(A)$ is the fixed-points subgroup and ${\rm Irr}_A(S)$ is the set of A-invariant irreducible characters of S. (See [Is3, Chapter 13].) Since the map is canonical, it is not difficult to see that $\mathbb{Q}(\theta) = \mathbb{Q}(\theta^*)$, where $\mathbb{Q}(\theta)$ is the field of values of θ. (See [Is3, Problem 3.1].)

Suppose now that $S = {}^2B_2(2^n)$, where n is odd. Then it is well-known that S admits a field automorphism a of order n. Assume further that $(m, |S|) = 1$ for some divisor $m > 1$ of n. Consider $A = \langle a^{n/m} \rangle \cong C_m$. If $m = n$, then $C = \mathbf{C}_S(A) = {}^2B_2(2) \cong C_5 \rtimes C_4$ has 5 irreducible characters; two of its four linear characters are rational, the others have field of values $\mathbb{Q}(i)$. It also has a rational irreducible character of degree 4. In particular, it follows that ${\rm Irr}(S)$ has exactly 5 irreducible A-invariant characters, and exactly two of them have field of values $\mathbb{Q}(i)$. On the other hand, if $m < n$, then $C = \mathbf{C}_S(A) = {}^2B_2(2^{n/m})$ has exactly 2 irreducible A-invariant characters with field of values $\mathbb{Q}(i)$, namely the ones of degree $(r-1)\sqrt{r/2}$ with $r := 2^{n/m}$; see [Bur]. This proves the following.

Lemma 9.1. *Suppose that $S = {}^2B_2(2^n)$, where n is odd. Assume further that $(m, |S|) = 1$ for a divisor $m > 1$ of n, and let A be the subgroup of field automorphisms of S of order m. Let $C = \mathbf{C}_S(A)$. If $\theta \in {\rm Irr}_A(S)$ has field of values $\mathbb{Q}(i)$, then θ^* has degree $(r-1)\sqrt{r/2}$ with $r := 2^{n/m}$.*

Lemma 9.2. *Suppose that A is a cyclic group of order m acting faithfully and coprimely on S. Let $\theta \in {\rm Irr}(S)$ be A-invariant, $C = \mathbf{C}_S(A)$, and let $\eta \in {\rm Irr}(C)$ be the A-Glauberman correspondent of θ. Let $G = S \rtimes A$ be the semidirect product, and let $\psi \in {\rm Irr}(G)$ be an extension of θ. Consider $x \in G \smallsetminus S$ such that $\langle x, S \rangle = G$.*

(i) *If η is linear, then $|\psi(x)| = 1$.*
(ii) *In all cases, there exist a root of unity $\gamma \in \mathbb{C}^\times$ of order dividing $2m$ and $c \in C$ such that $\psi(x) = \gamma\eta(c)$.*

Proof. Let $\psi \in {\rm Irr}(G)$ be the canonical extension of θ to G. (This is the unique extension ψ such that the determinantal order is coprime with $|A|$, see [Is3, Corollary 6.28]). Since every extension of θ to G is a multiple of ψ by a linear character λ of G/S, we may assume that $\psi = \lambda\psi_0$, where ψ_0 is the canonical extension.

Observe that m divides the order of x. Since m is coprime to $|S|$, we can write $x = cb = bc$, with b being a π-element and c being a π'-element, where π is the set of prime divisors of m. Also $|b| = m$, and $S \ni x^m = b^m c^m = c^m$, implying $c \in S$ since $\gcd(m, |S|) = 1$. Moreover, $G = S \rtimes \langle b \rangle$,

so without any loss we may replace A by $\langle b\rangle$, and now $c \in C = \mathbf{C}_S(b) = \mathbf{C}_S(A)$. By [Is3, Theorem 13.6]

$$\psi_0(x) = \psi_0(cb) = \epsilon\eta(c)\,,$$

where $\epsilon = \pm 1$. Hence, $\psi(x) = \gamma\eta(c)$, where $\gamma = \epsilon\lambda(x)$ and $\lambda(x)^m = 1$. □

Since each of the two irreducible characters of $S := {}^2B_2(q)$ of degree $(q-1)\sqrt{q/2}$ has field of values $\mathbb{Q}(i)$ and is $\mathrm{Aut}(S)$-invariant, Lemmas 9.1 and 9.2 imply the following.

Corollary 9.3. *Let $q = 2^n$ with $2 \nmid n$ and let θ be either of the two irreducible characters of $S := {}^2B_2(q)$ of degree $(q-1)\sqrt{q/2}$. Then θ extends to $G = \mathrm{Aut}(S) \cong S \rtimes C_n$. If furthermore n is coprime to $|S|$, then $|\psi(x)| = 1$ for any extension ψ of θ to G and for any $x \in G \smallsetminus S$ with $G = \langle x, S\rangle$.*

We remark that the character θ in Corollary 9.3 has a canonical extension to G. Indeed, by [N1, Theorem A], there exists a unique $\psi \in \mathrm{Irr}(G)$ such that the field of values of ψ is $\mathbb{Q}(i)$. In particular, notice that the restriction ψ to C_n is rational-valued.

In some non-coprime situations, we can use the following statement. This also follows from results in [Da, §9], but in the situation under consideration, our approach is more straightforward.

Lemma 9.4. *Suppose that $G = SA$, where $A = \langle a\rangle$, $S \lhd G$ and $A \cap S = 1$. Let $C = \mathbf{C}_S(A)$, and assume that $\chi \in \mathrm{Irr}_A(S)$ has an extension $\psi \in \mathrm{Irr}(G)$ such that ψ_A is rational-valued. Suppose that for every $x \in G \smallsetminus S$, there exists some $g \in G$ such that $x^g = cb$ for some $c \in C$ and $b \in A$. Then there exist a character $\theta \in \mathrm{Irr}(C)$ and a sign $\epsilon = \pm$ such that $\psi(cb) = \epsilon\theta(c)$ for every $c \in C$ and every generator b of A.*

Proof. By the proof of [Is3, Lemma 13.5], we can write

$$\psi_{CA} = \sum_{\beta\in\mathrm{Irr}(C),[\chi_C,\beta]\neq 0} \beta \boxtimes \psi_\beta\,,$$

where ψ_β is a rational-valued character of S. Now, define $\theta(c) = \psi(ca)$ for $c \in C$. Then

$$\theta = \sum_\beta \psi_\beta(s)\beta\,.$$

Thus θ is a virtual character of C. We claim that $[\theta,\theta] = 1$. Let T be a set of representatives for the right cosets of C in S. In order to use the proof of [Is3, Theorem 13.6], we claim that

$$Sa = \bigcup_{t\in T} (Ca)^t$$

is a disjoint union. By hypothesis,

$$Sa = \bigcup_{s\in S} (Ca)^s = \bigcup_{t\in T} (Ca)^t\,.$$

Now,

$$|S| = |Sa| = |\bigcup_{t\in T} (Ca)^t| \leq \sum_{t\in T} |(Ca)^t| = |T||C| = |S|\,,$$

and the claim follows. The rest of the proof follows as in [Is3, Theorem 13.6]. □

Finally, to address the general situation in the Suzuki case, we must go much deeper into [Da, §9].

Corollary 9.5. *Let $q = 2^n$ with $2 \nmid n$ and let θ be either of the two irreducible characters of $S := {}^2B_2(q)$ of degree $(q-1)\sqrt{q/2}$. Then θ extends to $G = \mathrm{Aut}(S) \cong S \rtimes C_n$ and $|\psi(x)| = 1$ for any extension ψ of θ to G and for any $x \in G \smallsetminus S$ with $G = \langle x, S\rangle$.*

Proof. We adapt the notation of [Da, §9] to ours. We know that $\mathbf{C}_S(A) = B \rtimes R$, where $B = \langle\beta\rangle$ has order 5, and R is a cyclic group of order 4. Now, let $G' = \mathbf{N}_G(B) = S' \rtimes A$, where $S' = \mathbf{N}_S(B)$. Let G_0 be the set of $x \in G$ such that $\langle xS\rangle = G/S$, and let G_0' be the set of $x \in G'$ such that $\langle xS'\rangle = G'/S'$. By [Da, Lemma 9.3], $S' = C \rtimes R$, where C is a cyclic group described there. By [Da, Proposition 9.7], G_0' is a trivial intersection subset of G with normalizer G'. In Dade's language, it satisfies (6.4) of [Da]. In particular, by [Da, Lemma 6.5],

$$G_0 = \bigcup_{\tau\in T} (G_0')^\tau$$

is a disjoint union, where $G = \bigcup_{\tau\in T} G'\tau$ is a disjoint union. (In that lemma right cosets are used.) In particular, if $x \in G_0'$ and η is a class function of G', then

$$\eta^G(x) = \eta(x)\,.$$

By [Da, Theorem 9.8], θ naturally corresponds to some irreducible character $\eta \in \mathrm{Irr}_A(S')$, which therefore has field of values $\mathbb{Q}(i)$. Now, S only has two A-invariant irreducible characters with field of values $\mathbb{Q}(i)$, so using the inverse of Dade's natural correspondence from that theorem, necessarily η is one of the two linear characters of $S'/C = R$.

By hypothesis $\langle x, S\rangle = G$, and so $x \in G_0$. Since

$$G_0 = \bigcup_{\tau\in T} (G_0')^\tau\,,$$

we may assume that $x \in G_0'$. By [Is2, Lemma G], $\psi(x) = \epsilon\gamma(x)$, where $\gamma \in \mathrm{Irr}(S'A)$ is an extension of η, and ϵ is a root of unity. In particular, γ is linear. We conclude that $|\psi(x)| = 1$, as desired. □

Lemma 9.6. *Let $S \lhd G < \mathrm{GL}(V) \cong \mathrm{GL}_d(\mathbb{C})$, where G is finite, $S = {}^2B_2(q)$, $D = q_0(q-1)$ with $q_0 = 2^n$, $q = 2^{2n+1}$, and $V = \mathbb{C}^D$ is irreducible over S. Suppose that G contains two elements g_0, g_1 such that $\mathrm{Trace}(g_0) = \pm i$, $\mathrm{Trace}(g_1) = \pm 1$, and $g_1 \in g_0S$. Suppose in addition that the trace of every element in $\mathbf{Z}(G)$ belongs to $\mathbb{Q}(i)$. Then g_0 and g_1 both induce non-inner automorphisms of S.*

Proof. Assume the contrary. As $g_1 \in g_0S$, g_0 induces an inner automorphism of S. Hence we can write $g_0 = zs$ for some $s \in S$ and some $z \in \mathbf{C}_G(S) = \mathbf{Z}(G)$. Since G is finite, z has finite order, whence $z = \zeta \cdot \mathrm{id}_V$ for some root of unity ζ. By assumption, $\zeta \in \mathbb{Q}(i)$, whence $\zeta^4 = 1$.

First suppose that $\zeta = \pm 1$. Then $\mathrm{Trace}(s) = \zeta^{-1}\mathrm{Trace}(g_0) = \pm i$, but this is impossible for any element in S, see [Suz]. Hence, $\zeta = \pm i$. Recalling that $g_1 \in g_0S$, we can write $g_1 = g_0t = zst$ for some $t \in S$. In such a case, $\mathrm{Trace}(st) = \zeta^{-1}\mathrm{Trace}(g_1) = \pm i$, and we again arrive at a contradiction since $st \in S$. □

9B. Traces of Frobenii and arithmetic monodromy groups. We now give a lemma on traces for those local systems $\mathcal{F}(q, f)$ in which the polynomial $f(x)$ of degree $(q_0+1)t(q)$ lies in $\mathbb{F}_2[x]$ and has $f(0) = 0$. Recall that $q_0 = 2^n$, $n \geq 1, q = 2q_0^2$, $t(q) = q + 1 - 2q_0$; for $k/\mathbb{F}_2$ a finite extension and $i = \zeta_4$, the trace function of $\mathcal{F}(q, f)$ is

$$t \in k \mapsto \frac{-1}{\big(1 - (-1)^n\, i\big)^{\deg(k/\mathbb{F}_2)}} \sum_{x\in k} \psi_2(\mathrm{Trace}_{W_2(k)/W_2(\mathbb{F}_2)}([x^{t(q)}, f(x) + tx])).$$

Lemma 9.7. *For $\mathcal{F}(q, f)$ as above, i.e. with $f(x) \in \mathbb{F}_2[x]$ of degree $(q_0+1)t(q)$ and $f(0) = 0$, define*

$$A := \text{ the number of nonzero monomials in } f(x),$$

so that $A \equiv f(1) \pmod 2$. *Then the traces at points of* $\mathbb{F}_2$ *are given as follows, with* $i = \zeta_4$*:*

$$\mathrm{Trace}\big(\mathrm{Frob}_{0,\mathbb{F}_2}|\mathcal{F}(q,f)\big) = \begin{cases} -1, & \text{if } 2 \nmid (A-n), \\ -(-1)^n i, & \text{if } 2|(A-n), \end{cases}$$
$$\mathrm{Trace}\big(\mathrm{Frob}_{1,\mathbb{F}_2}|\mathcal{F}(q,f)\big) = \begin{cases} -(-1)^n i, & \text{if } 2 \nmid (A-n), \\ -1, & \text{if } 2|(A-n). \end{cases}$$

Furthermore, for any finite extension $k/\mathbb{F}_2$ *and any* $t \in k$, $|\mathrm{Trace}(\mathrm{Frob}_{t,k}|\mathcal{F}(q,f))| \leq \sqrt{\#k}$.

Proof. The trace at time $0 \in \mathbb{F}_2$ is $\frac{-1}{(1-(-1)^n i)}$ times the sum

$$\psi_2[0,0] + \psi_2[1,A] = 1 + (-1)^A i,$$

while the trace at time $1 \in \mathbb{F}_2$ is $\frac{-1}{(1-(-1)^n i)}$ times the sum

$$\psi_2[0,0] + \psi_2[1,A+1] = 1 + (-1)^{A+1} i.$$

If $(-1)^A = -(-1)^n$, these traces are respectively -1 and $-(-1)^n i$. If $(-1)^A = (-1)^n$, these traces are respectively $-(-1)^n i$ and -1. For the second statement, note that $\mathrm{Trace}(\mathrm{Frob}_{t,k}|\mathcal{F}(q,f))$ is a sum of $\#k$ terms, each of absolute value 1, divided by a clearing factor of absolute value $\sqrt{\#k}$, hence it has absolute value $\leq \sqrt{\#k}$. □

Theorem 9.8. *Let* $n \in \mathbb{Z}_{\geq 1}$ *and* $q = 2^{2n+1}$. *Suppose the Airy sheaf* $\mathcal{F}(q,f)$ *defined in* (4.1.3) *with* $q = 2^{2n+1}$, $f(x) \in \mathbb{F}_2[x]$, *and* $f(0) = 0$, *has finite geometric monodromy group* S. *Then the following statements hold for* S *and the arithmetic monodromy group* $G := G_{\mathrm{arith},\mathbb{F}_2}$ *of* $\mathcal{F}(q,f)$ *over* $\mathbb{F}_2$.

(i) $S = {}^2B_2(q)$. *Furthermore,* G *induces non-inner automorphisms of* S, $G = \mathbf{Z}(G) \times R$ *for some* $S < R \leq \mathrm{Aut}(S) = S \rtimes C_{2n+1}$, *and* $\mathbf{Z}(G) \leq C_4$.

(ii) *If* $2n+1$ *is coprime to* $|S|$, *then* $G \cong \mathbf{Z}(G) \times \mathrm{Aut}(S)$.

(iii) *Suppose that* $|\mathrm{Trace}(\mathrm{Frob}_{0,\mathbb{F}_{q^2}})| = q_0 := 2^n$. *Then* $G \cong \mathbf{Z}(G) \times \mathrm{Aut}(S)$. *Moreover,* $|\mathbf{Z}(G)| \leq 2$ *if* $\mathrm{Trace}(\mathrm{Frob}_{0,\mathbb{F}_{q^2}}) = -q_0$ *or* $\mathrm{Trace}(\mathrm{Frob}_{0,\mathbb{F}_q}) = \pm q_0 i$, *and* $\mathbf{Z}(G) = 1$ *if* $\mathrm{Frob}_{1,\mathbb{F}_2}$ *has odd order.*

Proof. (i) By Theorem 8.4, the geometric monodromy group of $\mathcal{F}(q,f)$ is $S = {}^2B_2(q)$ in its irreducible representation of degree $D = q_0(q-1)$. By Lemma 9.7, for the images g_0 of $\mathrm{Frob}_{0,\mathbb{F}_2}$ and g_1 of $\mathrm{Frob}_{1,\mathbb{F}_2}$ in G, one has trace $\pm i$ and the other has trace ± 1. Note that $g_1 \in g_0 S$, and since G is finite, the traces of all elements in G belong to $\mathbb{Q}(i)$ by Chebotarev density. By Lemma 9.6, g_0 induces a non-inner automorphism of S.

Recall that $\mathrm{Out}(S) \cong C_{2n+1}$. Then G projects onto a subgroup $S \rtimes C_m$ of $\mathrm{Aut}(S)$ with kernel $\mathbf{C}_G(S) = \mathbf{Z}(G)$, for some divisor $m > 1$ of $2n+1$. Again, each element in $\mathbf{Z}(G)$ acts as a scalar α on $\mathbb{C}^D$ and has trace a root of unity belonging to $\mathbb{Q}(i)$, whence $\alpha^4 = 1$, and thus $\mathbf{Z}(G) \leq C_4$. Now $(G/S)/(\mathbf{Z}(G)S/S) \cong G/\mathbf{Z}(G)S \cong C_m$ is cyclic, and $\mathbf{Z}(G)/S \leq \mathbf{Z}(G/S)$. It follows that G/S is abelian of order $m|\mathbf{Z}(G)|$, with cyclic quotient of odd order m and a cyclic 2-subgroup $\mathbf{Z}(G)S/S$ of order $|\mathbf{Z}(G)|$. Hence $G/S = R/S \times \mathbf{Z}(G)/S$, with $R \cong S \rtimes C_m$. The composition factors of R are S and cyclic groups of odd order (dividing m), so $R \cap \mathbf{Z}(G) = 1$ and $G = \mathbf{Z}(G) \times R$.

(ii) Now assume that $2n+1$ is coprime to $|S|$, but $m < 2n+1$. Let ψ be the character of $R = S \rtimes C_m$ acting on the sheaf, which extends the character θ of S. Let η denote the Glauberman correspondent of θ as in Lemma 9.2, in particular, it has degree $(r-1)\sqrt{r/2}$ for $r := 2^{(2n+1)/m} \geq 8$. We can write $g_0 = zh_0$ and $g_1 = zh_1$ for some $h_0, h_1 \in R$ and $z \in \mathbf{Z}(G)$ (recall $g_0 S = g_1 S$). Now z acts as a root of unity β with $\beta^4 = 1$, and $\psi(h_j) = \gamma_j \eta(c_j)$ with $c_j \in C = {}^2B_2(r)$ and $\gamma_j^{2m} = 1$ for $j = 0, 1$ by Lemma 9.2. Since $\eta(c_j), \beta, \psi(g_j) \in \mathbb{Q}(i)$, we see that $\gamma_j \in \mathbb{Q}(i)$. But $\gamma_j^{2m} = 1$ and $2 \nmid m$, so $\gamma_j = \pm 1$.

Note that, since $r \geq 8$, the character η does not take value $\pm i$, see [Suz]. Without loss we may assume $\psi(g_0) = \pm 1$ and $\psi(g_1) = \pm i$. Now, if $\beta = \pm i$, then $\eta(g_0) = \psi(g_0)/(\beta\gamma_0) = \pm i$, which is impossible. On the other hand, if $\beta = \pm 1$, then $\eta(g_1) = \psi(g_1)/(\beta\gamma_1) = \pm i$, which is again impossible. Hence $m = 2n+1$, as stated.

(iii) By assumption, $|\varphi(g_0^{4n+2})| = q_0$, where φ is the character of G acting on $\mathcal{F}(q,f)$. Using $G = \mathbf{Z}(G) \times R$, we again write $g_0 = zh_0$ with $z \in \mathbf{Z}(G)$ acting on $\mathcal{F}(q,f)$ as a root of unity β, and $h_0 \in R$. Then $\mathbf{Z}(G) = \langle z \rangle$ since $G = \langle g_0, S\rangle$, and $\beta^4 = 1$. Now $s := h_0^{2n+1} \in S$ as $R/S \hookrightarrow C_{2n+1}$, and $|\varphi(s^2)| = q_0$. Checking the character table of S [Bur], we see that $|s^2| = 2$ or 4 and thus s is a 2-element. But every 2-element of S has order dividing 4, so $|s| = 4$. Hence we can write $|h_0| = 4e$ for some $e|(2n+1)$.

Suppose that $e < 2n+1$, whence $e \leq (2n+1)/3$. Then g_0^e is the image of $\mathrm{Frob}_{0,2^e}$, and so

$$q_0 = 2^n > 2^{(2n+1)/6} \geq 2^{e/2} \geq |\varphi(g_0^e)| = |\varphi(h_0^e)|$$

by Lemma 9.7. On the other hand, since $R/S \hookrightarrow C_{2n+1}$ and h_0^e has order 4, $h_0^e \in S$ and hence $|\varphi(h_0^e)| = q_0$, a contradiction. Thus $|h_0| = 4(2n+1)$. Note that $|\mathbf{C}_S(s^2)| = q^2$, hence $|\mathbf{C}_G(s^2)|$ has order dividing $q^2|\mathbf{Z}(G)| \cdot |R/S|$. But h_0 belongs to $\mathbf{C}_G(s^2)$ and has order $4(2n+1)$; thus $(2n+1)$ divides $|R/S|$ and so $R = \mathrm{Aut}(S)$.

Since $G = \langle g_1, S\rangle$, the assumption that the image g_1 of $\mathrm{Frob}_{1,\mathbb{F}_2}$ has odd order implies that $2 \nmid |G/S|$, and so $\mathbf{Z}(G) = 1$. Next suppose that $|\mathbf{Z}(G)| > 2$ but $\varphi(g_0^{4n+2}) = -q_0$ or $\varphi(g_0^{2n+1}) = \pm q_0 i$. Then $\beta = \pm i$. In the former case,

$$\varphi(g_0^{4n+2}) = \varphi(\beta^{4n+2}h_0^{4n+2}) = -\varphi(h_0^{4n+2}) = -\varphi(s^2),$$

and thus the involution $s^2 \in S$ has trace q_0, which is impossible, cf. [Bur]. In the latter case,

$$\varphi(g_0^{2n+1}) = \varphi(\beta^{2n+1}h_0^{4n+2}) = \pm i\varphi(h_0^{2n+1}) = \pm i\varphi(s),$$

and thus $s \in S$ has trace $\pm q_0$, which is again impossible, cf. [Bur]. □

Proposition 9.9. *We consider the sheaf $\mathcal{F}_q$, $q = 2^{2n+1}$, as defined in the Introduction. Thus $\mathcal{F}_q := \mathcal{F}(q,f)$ with $f(x) := f_1(x^{t(q)})$, $f_1(x) := \sum_{i=1}^n x^{1+2^i}$ as in (4.1.3). For a finite extension $k/\mathbb{F}_2$, define*

$$\mathrm{Ker}(k) := \big\{x \in k \ \mid \ \sum_{i=0}^{2n} x^{2^i} = 0\big\}.$$

Then we have the following results.

(i) *For any subfield k of $\mathbb{F}_{q^2}$, $|\mathrm{Trace}(\mathrm{Frob}_{0,k}|\mathcal{F}_q)|^2$ is either 0 or $\#\mathrm{Ker}(k)$.*
(ii) $|\mathrm{Trace}(\mathrm{Frob}_{0,\mathbb{F}_{q^2}}|\mathcal{F}_q)|^2 = \#\mathrm{Ker}(\mathbb{F}_{q^2}) = \#\mathrm{Ker}(\mathbb{F}_q) = q/2$.

Proof. We first observe that $\gcd(t(q), q^2-1) = 1$. To see this, note that $t(q) = q+1-2q_0$ divides q^2+1 (indeed $(q+1-2q_0)(q+1+2q_0) = q^2+1$), while $\gcd(q^2-1, q^2+1) = \gcd(q^2-1, 2) = 1$. Thus for any subfield k of of $\mathbb{F}_{q^2}$, the map $x \mapsto x^{t(q)}$ is bijective on k.

The sheaf $\mathcal{F}_q$ was built out of the Witt vector

$$\big[x^{t(q)}, \sum_{i=1}^n x^{t(q)(1+2^i)}\big].$$

Let us denote by $\mathcal{H}_q$ the sheaf built by the same recipe, with same clearing factor, out of the Witt vector

$$\big[x, \sum_{i=1}^n x^{1+2^i}\big].$$

Then for any subfield k of of $\mathbb{F}_{q^2}$

$$\mathrm{Trace}(\mathrm{Frob}_{0,k}|\mathcal{F}_q) = \mathrm{Trace}(\mathrm{Frob}_{0,k}|\mathcal{H}_q), \tag{9.9.1}$$

precisely because the map $x \mapsto x^{t(q)}$ is bijective on k.

Let us rewrite the input Witt vector for $\mathcal{H}_q$ as

$$\big[x, \sum_{i=1}^{n} x^{1+2^i}\big] = [x, xR(x)] \text{ with } R(x) := \sum_{i=1}^{n} x^{2^i}. \tag{9.9.2}$$

With this rewriting, we apply the idea of van der Geer-van der Vlugt, cf. [vG-vV, §5], as follows. Let us define

$$V(x) := [x, xR(x)]. \tag{9.9.3}$$

In Witt vector addition in $\mathbb{F}_2$-algebras, using the fact that $R(x)$ is an additive polynomial, we get

$$\begin{aligned} V(x+y) - V(x) - V(y) &= [x+y, (x+y)(R(x)+R(y))] + [x, xR(x)+x^2] + [y, yR(y)+y^2] \\ &= [y, (x+y)x + (x+y)(R(x)+R(y)) + xR(x) + x^2] + [y, yR(y)+y^2] \\ &= [0, y^2 + (x+y)x + (x+y)(R(x)+R(y)) + xR(x) + x^2 + yR(y) + y^2] \\ &= [0, xy + xR(y) + yR(x)] \\ &= [0, \langle x, y\rangle] \end{aligned}$$

for

$$\langle x, y\rangle := xy + xR(y) + yR(x). \tag{9.9.4}$$

The key point is that $\langle x, y\rangle$ on $k \times k$ is a symmetric $\mathbb{F}_2$-bilinear map to k, and $\mathrm{Trace}_{k/\mathbb{F}_2}(\langle x, y\rangle)$ is a symmetric $\mathbb{F}_2$-bilinear form on $k \times k$ as $\mathbb{F}_2$ vector space.

Then

$$|\mathrm{Trace}(\mathrm{Frob}_{0,k}|\mathcal{H}_q)|^2 = (1/\#k) \sum_{x,y\in k} \psi_2\big(\mathrm{Trace}_{k/\mathbb{F}_2}(V(x) - V(y))\big)$$

(by the shearing transformation $(x, y) \mapsto (x + y, y)$)

$$\begin{aligned} &= (1/\#k) \sum_{x,y\in k} \psi_2\big(\mathrm{Trace}_{k/\mathbb{F}_2}(V(x+y) - V(y))\big) \\ &= (1/\#k) \sum_{x,y\in k} \psi_2\big(\mathrm{Trace}_{k/\mathbb{F}_2}(V(x) + [0, \langle x, y\rangle])\big) \\ &= \sum_{x\in k} \psi_2\big(\mathrm{Trace}_{k/\mathbb{F}_2}(V(x))\big)\Big((1/\#k)\sum_{y\in k} \psi\big(\mathrm{Trace}_{k/\mathbb{F}_2}(\langle x, y\rangle)\big)\Big). \end{aligned}$$

The second summand vanishes unless the given $x \in k$ has $\mathrm{Trace}_{k/\mathbb{F}_2}(\langle x, y\rangle) = 0$ for all $y \in k$, in which case it is 1. But $x \in k$ has $\mathrm{Trace}_{k/\mathbb{F}_2}(\langle x, y\rangle) = 0$ for all $y \in k$ if and only if $x \in \mathrm{Ker}(k)$. To see this, note that for $x, y \in k$,

$$\langle x, y\rangle = xy + xR(y) + yR(x) = xy + \sum_{i=1}^{n} xy^{2^i} + \sum_{i=1}^{n} yx^{2^i}$$

has the same $\mathrm{Trace}_{k/\mathbb{F}_2}$ as $\big(x + \sum_{i=1}^{n} x^{1/2^i} + \sum_{i=1}^{n} x^{2^i}\big)y$. So by nondegeneracy of the trace, $x \in k$ has $\mathrm{Trace}_{k/\mathbb{F}_2}(\langle x, y\rangle) = 0$ for all $y \in k$ if and only if

$$x + \sum_{i=1}^{n} x^{1/2^i} + \sum_{i=1}^{n} x^{2^i} = 0, \text{ i.e. if and only if } \sum_{i=0}^{2n} x^{2^i} = 0.$$

Thus for k a subfield of $\mathbb{F}_{q^2}$,

$$\big|\mathrm{Trace}(\mathrm{Frob}_{0,k}\mathcal{H}_q)\big|^2 = \sum_{x\in\mathrm{Ker}(k)} \psi_2\big(\mathrm{Trace}_{k/\mathbb{F}_2}(V(x))\big).$$

To show (i), notice that on $\mathrm{Ker}(k)$, $x \mapsto \mathrm{Trace}_{k/\mathbb{F}_2}(V(x))$ is additive, i.e. it is a linear form on $\mathrm{Ker}(k)$. If it is nontrivial, the sum giving $|\mathrm{Trace}(\mathrm{Frob}_{0,k}\mathcal{H}_q)|^2$ vanishes. If it is trivial, this sum is $\#\mathrm{Ker}(k)$.

To show (ii), notice that for any $k \subseteq \overline{\mathbb{F}_2}$, $\mathrm{Ker}(k)$ is precisely the set of elements $x \in k \cap \mathbb{F}_q$ with $\mathrm{Trace}_{\mathbb{F}_q/\mathbb{F}_2}(x) = 0$. (Indeed, if $x \in \mathrm{Ker}(k)$, then

$$0 = \sum_{i=0}^{2n} F^i(x) = F\big(\sum_{i=0}^{2n} F^i(x)\big) = \sum_{i=1}^{2n+1} F^i(x),$$

and so $x = F^{2n+1}(x)$, i.e. $x \in \mathbb{F}_q$.) In particular, $\mathrm{Ker}(\mathbb{F}_{q^2}) = \mathrm{Ker}(\mathbb{F}_q)$ and $\#\mathrm{Ker}(\mathbb{F}_q) = q/2$. Now for $x \in \mathrm{Ker}(\mathbb{F}_{q^2})$ we have

$$\begin{aligned}
\mathrm{Trace}_{\mathbb{F}_{q^2}/\mathbb{F}_2}(V(x)) &= \mathrm{Trace}_{\mathbb{F}_q/\mathbb{F}_2}\big(\mathrm{Trace}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(V(x))\big)\\
&= \mathrm{Trace}_{\mathbb{F}_q/\mathbb{F}_2}(V(x) + V(x))\\
&= \mathrm{Trace}_{\mathbb{F}_q/\mathbb{F}_2}([0, x^2])\\
&= [0, \mathrm{Trace}_{\mathbb{F}_q/\mathbb{F}_2}(x^2)]\\
&= [0, 0],
\end{aligned}$$

precisely because every $x \in \mathrm{Ker}(\mathbb{F}_{q^2})$ is an element of $\mathbb{F}_q$ of trace zero. So we see directly that each of the summands in the sum giving $|\mathrm{Trace}(\mathrm{Frob}_{0,\mathbb{F}_{q^2}}|\mathcal{H}_q)|^2$ is simply 1. □

Proposition 9.10. *For $q = 2^{2n+1}$ and the Airy sheaf $\mathcal{F}_q$,*

$$\mathrm{Trace}(\mathrm{Frob}_{0,\mathbb{F}_q}|\mathcal{F}_q) = -\epsilon 2^n i,$$

where $\epsilon := (-1)^{n(n+1)/2}$ is the Jacobi symbol

$$\epsilon_{2n+1} = \left(\frac{2}{2n+1}\right) = \begin{cases} 1, & \text{if } 2n+1 \equiv \pm 1 \pmod 8,\\ -1, & \text{if } 2n+1 \equiv \pm 3 \pmod 8.\end{cases}$$

Proof. (i) Proposition 9.9 implies that $\mathrm{Trace}(\mathrm{Frob}_{0,\mathbb{F}_q}|\mathcal{F}_q)$ lies in $\mathbb{Z}[i]$ (because the only possible non-integrality is at the unique place of $\mathbb{Q}(i)$ over 2, where this trace and its complex conjugate have the same 2-adic ord). Furthermore, we can work with traces over $\mathcal{H}_q$ instead of $\mathcal{F}_q$.

Let us denote by F the absolute Frobenius $x \mapsto x^2$, and define

$$R_n(x) := \sum_{i=1}^{n} F^i(x), \quad V_n(x) := [x, xR_n(x)] = [x, x\big(\sum_{i=1}^{n} F^i(x)\big)].$$

Consider the non-normalized sum

$$\mathrm{RawTrace}(\mathrm{Frob}_{0,\mathbb{F}_q}|\mathcal{F}_q) := -\sum_{x\in\mathbb{F}_q} \psi_2\big(\mathrm{Trace}_{\mathbb{F}_q/\mathbb{F}_2}(V_n(x))\big),$$

so that

$$\mathrm{RawTrace}(\mathrm{Frob}_{0,\mathbb{F}_q}|\mathcal{F}_q) = (1 - (-1)^n i)^{2n+1}\mathrm{Trace}(\mathrm{Frob}_{0,\mathbb{F}_q}|\mathcal{F}_q).$$

(ii) To explain the idea of the proof, consider first the case when $2n+1$ is an odd prime p. Then $\mathbb{F}_{2^p}/\mathbb{F}_2$ has degree p, and $\mathbb{F}_{2^p} \smallsetminus \mathbb{F}_2$ is the disjoint union of F-orbits of length p. On each such F-orbit,

the value of $\mathrm{Trace}_{\mathbb{F}_q/\mathbb{F}_2}(V_n(x))$ is constant, and this constant value is then repeated p times as we sum over this orbit. So we have a congruence modulo $p\mathbb{Z}[i]$:

$$\begin{aligned}\mathrm{RawTrace}(\mathrm{Frob}_{0,\mathbb{F}_q}|\mathcal{F}_q) &\equiv -\sum_{x\in\mathbb{F}_2}\psi_2\big(\mathrm{Trace}_{\mathbb{F}_q/\mathbb{F}_2}(V_n(x))\big)\\ &\equiv -\psi_2\big(\mathrm{Trace}_{\mathbb{F}_q/\mathbb{F}_2}(V_n(0))\big)-\psi_2\big(\mathrm{Trace}_{\mathbb{F}_q/\mathbb{F}_2}(V_n(1))\big)\\ &\equiv -\psi_2\big(\mathrm{Trace}_{\mathbb{F}_q/\mathbb{F}_2}[0,0]\big)-\psi_2\big(\mathrm{Trace}_{\mathbb{F}_q/\mathbb{F}_2}[1,n]\big)\end{aligned}$$

(remembering that $\mathbb{F}_q/\mathbb{F}_2$ has odd degree p, and both $V_n(0), V_n(1)$ are already $\mathbb{F}_2$-rational)

$$\equiv -\psi_2(p[0,0])-\psi_2(p[1,(p-1)/2]) = -1-\psi_2([1,(p-1)/2])^p = -1-(i^{1+(p-1)})^p = -1-i^{p^2} = -1-i.$$

So when $2n+1=p$, we have a congruence modulo $p\mathbb{Z}[i]$:

$$(1-(-1)^{(p-1)/2}i)^p\mathrm{Trace}(\mathrm{Frob}_{0,\mathbb{F}_q}|\mathcal{F}_q)\equiv -1-i.$$

Multiplying both sides by $(1+(-1)^{(p-1)/2}i)^p$, we get a congruence modulo $p\mathbb{Z}[i]$:

$$2^p\mathrm{Trace}(\mathrm{Frob}_{0,\mathbb{F}_q}|\mathcal{F}_q)\equiv -(1+i)(1+(-1)^{(p-1)/2}i)^p.$$

If $p\equiv 1 \pmod 4$, the right side is

$$-(1+i)^{p+1} = -(2i)(2i)^{(p-1)/2} = -(2i)2^{(p-1)/2}i^{(p-1)/2}.$$

If $p\equiv 3 \pmod 4$, the right side is

$$-(1+i)(1-i)^p = -2(1-i)^{p-1} = -2(-2i)^{(p-1)/2} = 2^{(p+1)/2}i^{(p-1)/2}.$$

Recalling that $2^p\equiv 2 \pmod p$, and that $(p-1)/2=n$, we get a congruence modulo $p\mathbb{Z}[i]$:

$$\mathrm{Trace}(\mathrm{Frob}_{0,\mathbb{F}_q}|\mathcal{F}_q)\equiv\begin{cases}-i2^ni^{(p-1)/2}, & \text{if } p\equiv 1 \pmod 4,\\ 2^ni^{(p-1)/2}, & \text{if } p\equiv 3 \pmod 4.\end{cases}$$

Thus

$$\mathrm{Trace}(\mathrm{Frob}_{0,\mathbb{F}_q}|\mathcal{F}_q)\equiv -\epsilon_p 2^n i, \tag{9.10.1}$$

where ϵ_p is given by $i^{(p-1)/2}=(-1)^{(p-1)/4}=(-1)^{(p^2-1)/8}$ when $p\equiv 1 \pmod 4$, and by $i^{(p+1)/2}=(-1)^{(p+1)/4}=(-1)^{(p^2-1)/8}$ when $p\equiv 3 \pmod 4$. Thus in both cases ϵ_p is the Legendre symbol $\left(\frac{2}{p}\right)=(-1)^{(p^2-1)/8}$.

In view of Proposition 9.9, $\mathrm{Trace}(\mathrm{Frob}_{0,\mathbb{F}_q}|\mathcal{F}_q)$ is either 0 or an element of $\mathbb{Z}[i]$ of absolute value 2^n. It cannot be 0 because of (9.10.1). So it must be one of $\pm 2^n$ or $\pm 2^n i$. Of these four possibilities, only $-\epsilon_p 2^n i$ is congruent modulo $p\mathbb{Z}[i]$ to $-\epsilon_p 2^n i$ (this is just the statement that for an odd prime p, the four powers of i are distinct modulo $p\mathbb{Z}[i]$).

(iii) We now turn to the general case, where we proceed by induction on the total number (counting multiplicity) of primes dividing $2n+1$. Thus we write

$$2n+1=ps,\ s=2a+1,\ p=2b+1,\ \text{with } a,b\geq 1 \text{ and } p \text{ prime}.$$

We will need to deal with both $\mathcal{F}_{2^{ps}}$ and $\mathcal{F}_{2^s}$. To simplify notation, let us write

$$Q:=2^{ps},\ q':=2^s.$$

Here

$$ps=s(2b+1)=2bs+s=2(sb+a)+1.$$

The idea is that $\mathbb{F}_Q \smallsetminus \mathbb{F}_{q'}$ is the disjoint union of F^s-orbits, each of length p, and on each of these orbits, the value of $\mathrm{Trace}_{\mathbb{F}_Q/\mathbb{F}_2}(V_{sb+a}(x))$ is constant, and this constant value is then repeated p times as we sum over this orbit. Thus we get a congruence modulo $p\mathbb{Z}[i]$:

$$\mathrm{RawTrace}(\mathrm{Frob}_{0,\mathbb{F}_Q}|\mathcal{F}_Q) \equiv -\sum_{x\in\mathbb{F}_{q'}} \psi_2\big(\mathrm{Trace}_{\mathbb{F}_Q/\mathbb{F}_2}(V_{sb+a}(x))\big).$$

But for $x \in \mathbb{F}_{q'}$, the trace from $\mathbb{F}_Q$ down to $\mathbb{F}_{q'}$ is just multiplication by p, so

$$\mathrm{Trace}_{\mathbb{F}_Q/\mathbb{F}_2}(V_{sb+a}(x)) = \mathrm{Trace}_{\mathbb{F}_{q'}/\mathbb{F}_2}(pV_{sb+a}(x)).$$

Suppose first that b is even, i.e. that $p \equiv 1 \pmod 4$. Recall $4[x,y] = 0$. So for $x \in \mathbb{F}_{q'}$,

$$\begin{aligned} pV_{sb+a}(x) = V_{sb+a}(x) &= [x, xR_a(x) + x\big(\sum_{i=a+1}^{sb+a} F^i(x)\big)] \\ &= [x, xR_a(x) + x\big(b\mathrm{Trace}_{\mathbb{F}_{q'}/\mathbb{F}_2}(x)\big)] = [x, xR_a(x)] = V_a(x), \end{aligned}$$

where the last equality holds because b is even. So in this even b case,

$$\mathrm{RawTrace}(\mathrm{Frob}_{0,\mathbb{F}_Q}|\mathcal{F}_Q) \equiv \mathrm{RawTrace}(\mathrm{Frob}_{0,\mathbb{F}_a}|\mathcal{F}_{q'}) \pmod{p\mathbb{Z}[i]}.$$

Suppose now that b is odd, i.e. that $p \equiv -1 \pmod 4$. Then for $x \in \mathbb{F}_{q'}$,

$$\begin{aligned} pV_{sb+a}(x) = -V_{sb+a}(x) &= -[x, xR_a(x) + x\big(\sum_{i=a+1}^{sb+a} F^i(x)\big)] \\ &= -[x, xR_a(x) + x\mathrm{Trace}_{\mathbb{F}_{q'}/\mathbb{F}_2}(x)] = [x, xR_a(x) + x^2 + x\mathrm{Trace}_{\mathbb{F}_{q'}/\mathbb{F}_2}(x)] \\ &= [x, xR_a(x)] + [0, x^2 + x\mathrm{Trace}_{\mathbb{F}_{q'}/\mathbb{F}_2}(x)] = V_a(x) + [0, x^2 + x\mathrm{Trace}_{\mathbb{F}_{q'}/\mathbb{F}_2}(x)]. \end{aligned}$$

But the term $[0, x^2 + x\mathrm{Trace}_{\mathbb{F}_{q'}/\mathbb{F}_2}(x)]$ has

$$\mathrm{Trace}_{\mathbb{F}_{q'}/\mathbb{F}_2}\big([0, x^2 + x\mathrm{Trace}_{\mathbb{F}_{q'}/\mathbb{F}_2}(x)]\big) = [0, \mathrm{Trace}_{\mathbb{F}_{q'}/\mathbb{F}_2}\big(x^2 + x\mathrm{Trace}_{\mathbb{F}_{q'}/\mathbb{F}_2}(x)\big)] = [0,0],$$

where the last equality holds because $\mathrm{Trace}_{\mathbb{F}_{q'}/\mathbb{F}_2}(x^2) = \mathrm{Trace}_{\mathbb{F}_{q'}/\mathbb{F}_2}(x) = (\mathrm{Trace}_{\mathbb{F}_{q'}/\mathbb{F}_2}(x))^2$. So in this odd b case as well, also

$$\mathrm{RawTrace}(\mathrm{Frob}_{0,\mathbb{F}_Q}|\mathcal{F}_Q) \equiv \mathrm{RawTrace}(\mathrm{Frob}_{0,\mathbb{F}_a}|\mathcal{F}_{q'}) \pmod{p\mathbb{Z}[i]}.$$

We have shown that

$$(1-(-1)^{sb+a}i)^{ps}\mathrm{Trace}(\mathrm{Frob}_{0,\mathbb{F}_Q}|\mathcal{F}_Q) \equiv (1-(-1)^a i)^s \mathrm{Trace}(\mathrm{Frob}_{0,\mathbb{F}_{q'}}|\mathcal{F}_q) \pmod{p\mathbb{Z}[i]}. \tag{9.10.2}$$

By the induction hypothesis,

$$\mathrm{Trace}(\mathrm{Frob}_{0,\mathbb{F}_{q'}}|\mathcal{F}_{q'}) = -\epsilon_s 2^a i. \tag{9.10.3}$$

The clearing factors are invertible modulo $p\mathbb{Z}[i]$. We next show that the clearing factors are equal modulo $p\mathbb{Z}[i]$. Their ratio is

$$\frac{(1-(-1)^{sb+a}i)^{ps}}{(1-(-1)^a i)^s} = \frac{(1-(-1)^{sb+a}i)^{ps}(1+(-1)^a i)^s}{2^s}.$$

If b is odd, then $(p+1)/2$ is even, and this ratio is

$$\frac{(1+(-1)^a i)^{ps+s}}{2^s} = \frac{(2(-1)^a i)^{s(p+1)/2}}{2^s} = 2^{s(p-1)/2}((-1)^a i)^{s(p+1)/2} = 2^{s(p-1)/2} i^{s(p+1)/2}.$$

If $b = (p-1)/2$ is even, this ratio is

$$(1-(-1)^a i)^{(p-1)s} = (-2(-1)^a i)^{s(p-1)/2} = 2^{s(p-1)/2} i^{s(p-1)/2}.$$

Let $\chi_{p,\mathrm{quad}}$ be the quadratic character of $\mathbb{F}_p^\times$, so $2^{(p-1)/2} \equiv \chi_{p,\mathrm{quad}}(2) \pmod{p\mathbb{Z}[i]}$. As s is odd, the ratio of clearing factors modulo $p\mathbb{Z}[i]$ is $\chi_{p,\mathrm{quad}}(2) i^{s(p-1)/2}$ when $p \equiv 1 \pmod 4$, and $\chi_{p,\mathrm{quad}}(2) i^{s(p+1)/2}$ when $p \equiv 3 \pmod 4$. Next, when $p \equiv 1 \pmod 4$,

$$i^{(p-1)/2} = \chi_{p,\mathrm{quad}}(2).$$

When $p \equiv 3 \pmod 4$,

$$i^{(p+1)/2} = \chi_{p,\mathrm{quad}}(2).$$

As s is odd, we find that in all cases the ratio of clearing factors is $1 \pmod{p\mathbb{Z}[i]}$, as stated. Hence (9.10.2) and (9.10.3) imply the congruence

$$\mathrm{Trace}(\mathrm{Frob}_{0,\mathbb{F}_Q} | \mathcal{F}_Q) \equiv \mathrm{Trace}(\mathrm{Frob}_{0,\mathbb{F}_{q'}} | \mathcal{F}_{q'}) = -\epsilon_s 2^a i \pmod{p\mathbb{Z}[i]}.$$

Note that

$$2^{sb} = (2^{(p-1)/2})^s \equiv \chi_{p,\mathrm{quad}}(2)^s = \chi_{p,\mathrm{quad}}(2) = \epsilon_p \pmod p.$$

Hence

$$\epsilon_{ps} 2^{sb+a} \equiv \epsilon_{ps}\epsilon_p 2^a = \epsilon_s 2^a \pmod p$$

by multiplicativity of the Jacobi symbol. It follows that

$$\mathrm{Trace}(\mathrm{Frob}_{0,\mathbb{F}_Q} | \mathcal{F}_Q) \equiv -\epsilon_{ps} 2^{sb+a} i \pmod{p\mathbb{Z}[i]}.$$

This congruence shows that $\mathrm{Trace}(\mathrm{Frob}_{0,\mathbb{F}_Q} | \mathcal{F}_Q)$ is nonzero, so by Proposition 9.9 it is one of $\pm 2^{sb+a}$ or $\pm 2^{sb+a} i$. Again, of these four possibilities, only $-\epsilon_{ps} 2^n i$ is congruent modulo $p\mathbb{Z}[i]$ to $-\epsilon_{ps} 2^n i$, and the induction step is complete. □

Proposition 9.11. *For $q = 2^{2n+1}$, consider the Airy sheaf $\mathcal{F}_q$. Then for any subfield k of $\mathbb{F}_q$*

$$|\mathrm{Trace}(\mathrm{Frob}_{1,k} | \mathcal{F}_q)|^2 = 1.$$

Proof. Let k be a subfield of $\mathbb{F}_{q^2}$. Note that $N := (q + 2q_0 + 1)q^2/2$ divides $(q^2+1)q^2$ and so is coprime to q^2-1. Hence the map $x \to x^N$ is a bijection on k, and it sends $x^{t(q)}$ to $x^{(q^2+1)q^2/2} = x$ for any $x \in k$. As in the proof of Proposition 9.10, let us denote by F the absolute Frobenius $x \mapsto x^2$. For each integer $j \geq 0$, we define

$$R_j(x) := \sum_{i=1}^{j} F^i(x).$$

Consider the non-normalized sum

$$\mathrm{RawTrace}(\mathrm{Frob}_{1,k} | \mathcal{F}_q) := -\sum_{x \in k} \psi_2\big(\mathrm{Trace}_{k/\mathbb{F}_2}(V(x))\big),$$

where $V(x) = [x, xR_n(x) + x^N]$. Then we have

$$\mathrm{RawTrace}(\mathrm{Frob}_{1,k} | \mathcal{F}_q) = (1-(-1)^n i)^{\deg(k/\mathbb{F}_2)} \mathrm{Trace}(\mathrm{Frob}_{1,k} | \mathcal{F}_q).$$

We now take k to be a subfield of $\mathbb{F}_q$. We examine the function $x \mapsto x^N$ on k. This function depends only on $N \pmod{(q-1)}$. Then

$$N \equiv (1 + 1 + 2q_0)q/2 = (2 + 2q_0)q/2 = q + qq_0 \equiv 1 + q_0 = 1 + 2^n \pmod{(q-1)}.$$

Thus if $x \in k$, then $x^N = xF^n(x)$, and hence

$$V(x) = [x, xR_n(x) + x^N] = [x, xR_n(x) + xF^n(x)] = [x, xR_{n-1}(x)].$$

At this point, we repeat the van der Geer-van der Vlugt argument of Theorem 9.9. We find that if k is a subfield of $\mathbb{F}_q$, then

$$|\mathrm{Trace}(\mathrm{Frob}_{1,k}|\mathcal{F}_q)|^2 = \sum_{x\in \mathrm{Ker}'(k)} \psi_2\big(\mathrm{Trace}_{k/\mathbb{F}_2}(V(x))\big),$$

with

$$\mathrm{Ker}'(k) := \big\{x \in k | \sum_{i=0}^{2n-2} F^i(x) = 0\big\}.$$

The key observation is that for k a subfield of $\mathbb{F}_q$, $\mathrm{Ker}'(k) = \{0\}$. Indeed, since

$$0 \in \mathrm{Ker}'(k) \subseteq \mathrm{Ker}'(\mathbb{F}_q),$$

it suffices to show that $\mathrm{Ker}'(\mathbb{F}_q) = \{0\}$. But for $x \in \mathrm{Ker}'(\mathbb{F}_q)$,

$$\mathrm{Trace}_{\mathbb{F}_q/\mathbb{F}_2}(x) = \big(\sum_{i=0}^{2n-2} F^i(x)\big) + F^{2n-1}(x) + F^{2n}(x) = F^{2n-1}(x) + F^{2n}(x).$$

Thus for $x \in \mathrm{Ker}'(\mathbb{F}_q)$, $\mathrm{Trace}_{\mathbb{F}_q/\mathbb{F}_2}(x) = F^{2n-1}(x + F(x))$. As $\mathrm{Trace}_{\mathbb{F}_q/\mathbb{F}_2}(x) \in \mathbb{F}_2$, this gives

$$\mathrm{Trace}_{\mathbb{F}_q/\mathbb{F}_2}(x) = x + x^2.$$

If $\mathrm{Trace}_{\mathbb{F}_q/\mathbb{F}_2}(x) = 0$, then $x + x^2 = 0$, i.e. $x \in \mathbb{F}_2$, so x is 0 or 1. Of these, only $x = 0$ has $\mathrm{Trace}_{\mathbb{F}_q/\mathbb{F}_2}(x) = 0$. If $\mathrm{Trace}_{\mathbb{F}_q/\mathbb{F}_2}(x) = 1$, then $x + x^2 = 1$ and so $\mathbb{F}_2(x) = \mathbb{F}_4$. But $\mathbb{F}_4$ is not a subfield of $\mathbb{F}_q$, which has odd degree $2n + 1$ over $\mathbb{F}_2$. So in this second case, there are no possible x.

Thus

$$\big|\mathrm{Trace}(\mathrm{Frob}_{1,k}|\mathcal{F}_q)\big|^2 = \sum_{x\in \mathrm{Ker}'(k)} \psi_2\big(\mathrm{Trace}_{k/\mathbb{F}_2}(V(x))\big) = \psi_2(\mathrm{Trace}_{k/\mathbb{F}_2}(V(0))) = \psi_2([0,0]) = 1.$$

□

Proposition 9.12. *For $q = 2^{2n+1}$ and the Airy sheaf $\mathcal{F}_q$,*

$$\mathrm{Trace}(\mathrm{Frob}_{1,\mathbb{F}_q}|\mathcal{F}_q) = -1.$$

Proof. (i) The quantity $\mathrm{Trace}(\mathrm{Frob}_{1,k}|\mathcal{F}_q)$ lies in $\mathbb{Q}(i)$ and is integral outside the unique place over 2, so by Proposition 9.11, $\mathrm{Trace}(\mathrm{Frob}_{1,\mathbb{F}_q}|\mathcal{F}_q)$ is one of $\{1, -1, i, -i\}$. For any odd prime p, these four elements are distinct modulo $p\mathbb{Z}[i]$. We proceed by induction on the total number (counting multiplicity) of primes in the factorization of $2n + 1$.

For the induction base, suppose that $k = \mathbb{F}_q = \mathbb{F}_{2^p}$. Then $\mathbb{F}_q \smallsetminus \mathbb{F}_2$ is the disjoint union of F-orbits of length divisible by p. On each such F-orbit, the value of $\mathrm{Trace}_{\mathbb{F}_q/\mathbb{F}_2}(V(x))$ is constant, and this constant value is then repeated a multiple of p times as we sum over this orbit. So we have a congruence modulo $p\mathbb{Z}[i]$:

$$\begin{aligned}
\mathrm{RawTrace}(\mathrm{Frob}_{1,\mathbb{F}_q}|\mathcal{F}_q) &\equiv -\sum_{x\in\mathbb{F}_2} \psi_2\big(\mathrm{Trace}_{\mathbb{F}_q/\mathbb{F}_2}(V(x))\big) \\
&\equiv -\psi_2\big(\mathrm{Trace}_{\mathbb{F}_q/\mathbb{F}_2}(V(0))\big) - \psi_2\big(\mathrm{Trace}_{\mathbb{F}_q/\mathbb{F}_2}(V(1))\big) \\
&\equiv -\psi_2\big(\mathrm{Trace}_{\mathbb{F}_q/\mathbb{F}_2}[0,0]\big) - \psi_2\big(\mathrm{Trace}_{\mathbb{F}_q/\mathbb{F}_2}[1,n+1]\big) \\
&\equiv -\psi_2(s[0,0]) - \psi_2(p[1,(p+1)/2]) = -1 - \psi_2([1,(p+1)/2])^p \\
&= -1 - (i^{1+(p+1)})^p = -1 - i^{p^2+2p} = -1 + i.
\end{aligned}$$

So for $\mathrm{Frob}_{1,\mathbb{F}_q}$, we have a congruence modulo $p\mathbb{Z}[i]$:

$$(1-(-1)^{(p-1)/2}i)^p\mathrm{Trace}(\mathrm{Frob}_{1,\mathbb{F}_q}|\mathcal{F}_q) = \mathrm{RawTrace}(\mathrm{Frob}_{1,\mathbb{F}_q}|\mathcal{F}_q) \equiv -1+i.$$

Multiplying both sides by $(1+(-1)^{(p-1)/2}i)^p$, we get a congruence modulo $p\mathbb{Z}[i]$:

$$2^p\mathrm{Trace}(\mathrm{Frob}_{0,\mathbb{F}_q}|\mathcal{F}_q) \equiv -(1-i)(1+(-1)^{(p-1)/2}i)^p.$$

If $p \equiv 3 \pmod 4$, the right side is

$$-(1-i)^{p+1} = -(2i)^{(p+1)/2} = -2^{(p+1)/2}(-1)^{(p+1)/4} \equiv -2(-1)^{(p^2-1)/8+(p+1)/4} = -2 \pmod p.$$

If $p \equiv 1 \pmod 4$, the right side is $-(1-i)(1+i)^p$, which is

$$-2(1+i)^{s-1} = -2(2i)^{(p-1)/2} = -2^{(p+1)/2}(-1)^{(p-1)/4} \equiv -2(-1)^{(p^2-1)/8+(p-1)/4} = -2 \pmod p.$$

Thus in both cases $q\mathrm{Trace}(\mathrm{Frob}_{1,\mathbb{F}_q}|\mathcal{F}_q) \equiv -2 \pmod{p\mathbb{Z}[i]}$. Using Proposition 9.11, we conclude that $\mathrm{Trace}(\mathrm{Frob}_{1,\mathbb{F}_q}|\mathcal{F}_q) = -1$ in this case.

(ii) Suppose now that $2n+1 = ps$ with an odd prime p and an odd integer s. Then just as in (iii) of the proof of Proposition 9.10 we write

$$s = 2a+1,\ p = 2b+1,\ ps = 2(sb+a)+1.$$

We will need to deal with both $\mathcal{F}_{2^{ps}}$ and $\mathcal{F}_{2^s}$. To simplify notation, let us write

$$Q := 2^{ps},\ q' := 2^s.$$

Then, just as in the proof of Proposition 9.11,

$$\mathrm{RawTrace}(\mathrm{Frob}_{1,\mathbb{F}_Q}|\mathcal{F}_Q) = -\sum_{x\in\mathbb{F}_Q}\psi_2(\mathrm{Trace}_{\mathbb{F}_Q/\mathbb{F}_2}([x,R_{sb+a-1}(x)])).$$

The elements of $\mathbb{F}_Q \smallsetminus \mathbb{F}_{q'}$ fall into F-orbits of length p, and the elements from each of these orbits have the same $\mathrm{Trace}_{\mathbb{F}_Q/\mathbb{F}_2}([x,R_{sb+a-1}(x)])$. So we get a congruence modulo $p\mathbb{Z}[i]$

$$\begin{aligned}\mathrm{RawTrace}(\mathrm{Frob}_{1,\mathbb{F}_Q}|\mathcal{F}_Q) &\equiv -\sum_{x\in\mathbb{F}_{q'}}\psi_2(\mathrm{Trace}_{\mathbb{F}_Q/\mathbb{F}_2}([x,R_{sb+a-1}(x)]))\\ &= -\sum_{x\in\mathbb{F}_{q'}}\psi_2(\mathrm{Trace}_{\mathbb{F}_{q'}/\mathbb{F}_2}(p[x,R_{sb+a-1}(x)])).\end{aligned}$$

Notice that for $x \in \mathbb{F}_{q'}$,

$$R_{sb+a-1}(x) = R_{a-1}(x) + b\mathrm{Trace}_{\mathbb{F}_{q'}/F_2}(x).$$

Suppose first that $p \equiv 1 \pmod 4$. Then b is even,

$$p[x,R_{sb+a-1}(x)] = [x,R_{sb+a-1}(x)] = [x,xR_{a-1}(x)],$$

and hence

$$\mathrm{RawTrace}(\mathrm{Frob}_{1,\mathbb{F}_Q}|\mathcal{F}_Q) \equiv \mathrm{RawTrace}(\mathrm{Frob}_{1,\mathbb{F}_{q'}}|\mathcal{F}_{q'}) \pmod{p\mathbb{Z}[i]}$$

when $p \equiv 1 \pmod 4$.

Suppose next that $p \equiv -1 \pmod 4$. Since b is odd,

$$\begin{aligned}p[x,R_{sb+a-1}(x)] &= -[x,R_{sb+a-1}(x)] = [x,x^2+R_{sb+a-1}(x)]\\ &= [x,x^2+x\mathrm{Trace}_{\mathbb{F}_{q'}/\mathbb{F}_2}(x)+xR_{a-1}(x)]\\ &= [x,xR_{a-1}(x)]+[0,x^2+x\mathrm{Trace}_{\mathbb{F}_{q'}/\mathbb{F}_2}(x)].\end{aligned}$$

But for $x \in \mathbb{F}_{q'}$, $\mathrm{Trace}_{\mathbb{F}_{q'}/\mathbb{F}_2}$ annihilates $x^2 + x\mathrm{Trace}_{\mathbb{F}_{q'}/\mathbb{F}_2}(x)$, so again

$$\mathrm{RawTrace}(\mathrm{Frob}_{1,\mathbb{F}_Q}|\mathcal{F}_Q) \equiv \mathrm{RawTrace}(\mathrm{Frob}_{1,\mathbb{F}_{q'}}|\mathcal{F}_{q'}) \pmod{p\mathbb{Z}[i]}$$

when $p \equiv -1 \pmod 4$.

It remains only to show that the ratio of clearing factors is $1 \pmod{p\mathbb{Z}[i]}$ in both cases. When $p \equiv 1 \pmod 4$, $(p-1)/2$ is even, and this ratio is

$$\begin{aligned}(1-(-1)^a i)^{ps}/(1-(-1)^a i)^s = (1-(-1)^a i)^{(p-1)s} &= (-2(-1)^a i)^{s((p-1)/2)} \\ &= \big(2^{(p-1)/2}(-1)^{(p-1)/4}\big)^s \equiv 1 \pmod p,\end{aligned}$$

since $2^{(p-1)/2} \equiv (-1)^{(p^2-1)/8} \pmod p$. When $p \equiv -1 \pmod 4$, $(p+1)/2$ is even, and the ratio is

$$\begin{aligned}(1+(-1)^a i)^{ps}/(1-(-1)^a i)^s = (1+(-1)^a i)^{ps}(1+(-1)^a i)^s/2^s &= (1+(-1)^a i)^{(p+1)s}/2^s \\ = (2(-1)^a i)^{s(p+1)/2}/2^s &= \big(2^{(p-1)/2}(-1)^{(p+1)/4}\big)^s \equiv 1 \pmod p,\end{aligned}$$

again because $2^{(p-1)/2} \equiv (-1)^{(p^2-1)/8} \pmod p$. □

Lemma 9.13. *For $q = 2^{2n+1}$ and $S := {}^2B_2(q)$, suppose that $s \in \mathrm{Aut}(S)$ has odd order and that $\langle s, S\rangle = \mathrm{Aut}(S)$. Then $|s|$ divides $5(2n+1)$.*

Proof. Let $\mathcal{G} := \mathrm{Sp}_4(\overline{\mathbb{F}_2})$. It is well known that there is a Steinberg endomorphism $\sigma : \mathcal{G} \to \mathcal{G}$ such that σ^2 is the standard Frobenius map $(a_{ij}) \mapsto (a_{ij}^2)$ on $\mathcal{G}$, and then we can identify S with $\mathcal{G}^{\sigma^{2n+1}} := \{X \in \mathcal{G} \mid \sigma^{2n+1}(X) = X\}$, which is then σ-invariant. Letting σ also denote its action on S, we can write $\mathrm{Aut}(S) = \langle \sigma, S\rangle$. Without loss, we may assume $Ss = S\sigma^{-1}$, and write $s = x\sigma^{-1}$. By the Lang-Steinberg theorem, there is some $a \in \mathcal{G}$ such that

$$x = a\sigma(a)^{-1}. \tag{9.13.1}$$

We also note that in $\mathrm{Aut}(S)$

$$\big(x\sigma^{-1}\big)^{2n+1} = x \cdot \sigma(x) \cdot \sigma^2(x) \cdot \ldots \cdot \sigma^{2n}(x). \tag{9.13.2}$$

As in the proof of [GMPS, Theorem 2.16], define $t := a^{-1}s^{(2n+1)}a = \big(x\sigma^{-1}\big)^{2n+1}a$. Then using (9.13.1) and (9.13.2) we obtain

$$\begin{aligned}\sigma(t) &= \sigma(a)^{-1} \cdot \big(\sigma(x) \cdot \sigma^2(x) \cdot \ldots \cdot \sigma^{2n}(x) \cdot \sigma^{2n+1}(x)\big)\sigma(a) \\ &= \big(\sigma(a)^{-1}x^{-1}\big) \cdot \big(x \cdot \sigma(x) \cdot \ldots \cdot \sigma^{2n}(x)\big) \cdot \big(x\sigma(a)\big) \\ &= a^{-1}\big(x\sigma^{-1}\big)^{2n+1}a = t.\end{aligned}$$

Thus $t \in \mathcal{G}^\sigma \cong {}^2B_2(2)$, and note that $|{}^2B_2(2)| = 20$. Since s has odd order and t, s^{2n+1} are conjugate in $\mathcal{G}$, $|t|$ is odd, whence $|s^{2n+1}| = |t|$ divides 5. Thus $|s|$ divides $5(2n+1)$, as stated. □

Theorem 9.14. *Suppose the Airy sheaf $\mathcal{F}_q$ for $q = 2^{2n+1}$ has finite geometric monodromy group G_{geom}. Then the following statements hold.*

(i) *The arithmetic monodromy group over $\mathbb{F}_2$ of $\mathcal{F}_q$ is $G_{\mathrm{arith},\mathbb{F}_2} = C \times \mathrm{Aut}({}^2B_2(q))$, with $|C| \le 2$.*
(ii) *Moreover, $C = 1$ if $2n+1 \equiv \pm 3 \pmod 8$, and $C \cong C_2$ if $2n+1 \equiv \pm 1 \pmod 8$.*
(iii) *Suppose $2n+1 \equiv \pm 3 \pmod 8$. For the arithmetic monodromy group $G_{\mathrm{arith},k}$ of $\mathcal{F}_q$ over a finite extension $k/\mathbb{F}_2$, we have $G_{\mathrm{arith},\mathbb{F}_2} = \mathrm{Aut}({}^2B_2(q))$, $G_{\mathrm{arith},k} = G_{\mathrm{geom}} = {}^2B_2(q)$ when $k \supseteq \mathbb{F}_q$, and $[G_{\mathrm{arith},k} : G_{\mathrm{geom}}] = \deg(\mathbb{F}_q/k)$ when $k \subseteq \mathbb{F}_q$.*
(iv) *Suppose $2n+1 \equiv \pm 1 \pmod 8$.*

(α) *For the arithmetic monodromy group $G_{\mathrm{arith},k}$ of $\mathcal{F}_q$ over a finite extension $k/\mathbb{F}_2$, we have $G_{\mathrm{arith},k} = G_{\mathrm{geom}} = {}^2B_2(q)$ when $k \supseteq \mathbb{F}_{q^2}$, and $[G_{\mathrm{arith},k} : G_{\mathrm{geom}}] = \deg(\mathbb{F}_{q^2}/k)$ when $k \subseteq \mathbb{F}_{q^2}$.*

(β) *For the arithmetic monodromy group $G_{\mathrm{arith},\tilde{\mathcal{F}}_q,k}$ of the sheaf $\tilde{\mathcal{F}}_q := \mathcal{F}_q \otimes (-1)^{\deg/\mathbb{F}_2}$ over $k/\mathbb{F}_2$, we have $G_{\mathrm{arith},\tilde{\mathcal{F}}_q,\mathbb{F}_2} = \mathrm{Aut}({}^2B_2(q))$, $G_{\mathrm{arith},\tilde{\mathcal{F}}_q,k} = G_{\mathrm{geom},\tilde{\mathcal{F}}_q} = {}^2B_2(q)$ when $k \supseteq \mathbb{F}_q$, and $[G_{\mathrm{arith},\tilde{\mathcal{F}}_q,k} : G_{\mathrm{geom},\tilde{\mathcal{F}}_q}] = \deg(\mathbb{F}_q/k)$ when $k \subseteq \mathbb{F}_q$.*

Proof. Part (i) follows from Propositions 9.9, 9.10, and Theorem 9.8(iii).

(ii) Let g denote the image of $\mathrm{Frob}_{1,\mathbb{F}_2}$ in $G_{\mathrm{arith},\mathbb{F}_2}$. As $\langle g, G_{\mathrm{geom}}\rangle = C \times \mathrm{Aut}(S)$ for $S := {}^2B_2(q)$, we can write $g = zs$ with $C = \langle z\rangle \leq C_2$ and $s \in \mathrm{Aut}(S) \cong S \rtimes C_{2n+1}$. The central element z acts on $\mathcal{F}_q$ as the scalar ξ, where $\xi = 1$ if $|C| = 1$ and $\xi = -1$ if $|C| = 2$. The finiteness of G_{geom} implies that $G_{\mathrm{arith},\mathbb{F}_2}$ is finite, and so $\mathrm{Trace}(g^m)$ is a Gaussian integer for any $m \in \mathbb{Z}$. Now Proposition 9.12 implies that

$$\mathrm{Trace}(s^{2n+1}) = \xi\mathrm{Trace}(g^{2n+1}) = -\xi, \tag{9.14.1}$$

and note that $t := s^{2n+1} \in S$.

Also note that since $\mathrm{Aut}(S) = \langle s, S\rangle$, s has order $2n+1$ modulo S, whence $|s| = e(2n+1)$ for some $e \in \mathbb{Z}_{\geq 1}$, whence $|t| = e$. Inspecting the character table of S [Bur] and using (9.14.1), we see that $e = |t|$ is odd and greater than 1; in fact e divides $q - 2q_0 + 1$ if $\xi = 1$ and e divides $q + 2q_0 + 1$ if $\xi = -1$, where $q_0 := 2^n$. It follows that $|s| = e(2n+1)$ is odd. By Lemma 9.13, $e > 1$ divides 5, so $e = 5$; in particular, $|s| = 5(2n+1)$. An easy computation shows that $5|(q - 2q_0 + 1)$ precisely when $n \equiv 1, 2 \pmod 4$ (equivalently, $2n+1 \equiv \pm 3 \pmod 8$), and $5|(q + 2q_0 + 1)$ precisely when $n \equiv 0, 3 \pmod 4$ (equivalently, $2n+1 \equiv \pm 1 \pmod 8$). Hence the statement follows, and we have also proved that the image g of $\mathrm{Frob}_{1,\mathbb{F}_2}$ has order

$$\begin{cases} 10(2n+1), & \text{if } 2n+1 \equiv \pm 1 \pmod 8, \\ 5(2n+1), & \text{if } 2n+1 \equiv \pm 3 \pmod 8. \end{cases} \tag{9.14.2}$$

Parts (iii) and (iv)(α) follow from (i), (ii), and the facts that $G_{\mathrm{geom}} = {}^2B_2(q)$ and $G_{\mathrm{arith},\mathbb{F}_2}/G_{\mathrm{geom}}$ is cyclic of order $|C|(2n+1)$.

To prove (iv)(β), note that when $k \supseteq \mathbb{F}_4$, the images of $\pi_1(\mathbb{A}^1/k)$ on $\mathcal{F}_q$ and $\tilde{\mathcal{F}}_q$ are the same. Hence $G_{\mathrm{arith},\tilde{\mathcal{F}}_q,k} = G_{\mathrm{arith},k} = {}^2B_2(q)$ whenever $k \supseteq \mathbb{F}_{q^2}$, whence $G_{\mathrm{geom},\tilde{\mathcal{F}}_q} = {}^2B_2(q) = S$. Now $G_{\mathrm{arith},\tilde{\mathcal{F}}_q,\mathbb{F}_2} = \langle \tilde{g}, S\rangle$, where $\tilde{g}$ is the image of $\mathrm{Frob}_{1,\mathbb{F}_2}$ on $\tilde{\mathcal{F}}_q$. By its definition, $\tilde{g} = -g$, where g is the image of $\mathrm{Frob}_{1,\mathbb{F}_2}$ on $\mathcal{F}_q$, and the proof of (ii) shows (recalling $2n+1 \equiv \pm 1 \pmod 8$) that $g = -s$ with $\mathrm{Aut}(S) = \langle s, S\rangle$. Hence $G_{\mathrm{arith},\tilde{\mathcal{F}}_q,\mathbb{F}_2} = \langle s, S\rangle = \mathrm{Aut}(S) = S \rtimes C_{2n+1}$, and the assertion follows. □

Remark 9.15. Computations in MAGMA suggest that, for the Airy sheaf $\mathcal{F}_q$ with $q = 2^{2n+1}$, the Frobenii $\mathrm{Frob}_{a,\mathbb{F}_{2^j}}$ with $a \in \mathbb{F}_{2^j}$ and $\gcd(j, 2n+1) = 1$, all have traces of absolute value 1. If one knew that $\mathcal{F}_q$ has geometric monodromy group $G_{\mathrm{geom},\mathcal{F}_q} = {}^2B_2(q)$, then this "absolute value one" property agrees with Corollary 9.5. Also, for $n = 1, 2$, computations show that $\mathrm{Frob}_{1,\mathbb{F}_2}$ has order $5(2n+1)$, and this again agrees with (9.14.2).

On the other hand, the infinite case of the dichotomy, namely $G_{\mathrm{geom}} = \mathrm{SL}_D$ would imply by Deligne's equidistribution theorem [KaS, Theorem 9.7.13] that when j is large enough (compared to q), some (in fact most) Frobenii $\mathrm{Frob}_{a,\mathbb{F}_{2^j}}$ would have traces of absolute value $\neq 1$. This again gives some evidence in support of the geometric part of [Ka5, Conjecture 2.2] asserting that $G_{\mathrm{geom},\mathcal{F}_q} = {}^2B_2(q)$. However, Theorem 9.14(iii) shows that the arithmetic part of [Ka5, Conjecture 2.2] stating

that $G_{\mathrm{arith},\mathcal{F}_q,\mathbb{F}_2} = \mathrm{Aut}({}^2B_2(q))$ is false when $q = 2^m$ with $m \equiv \pm 1 \pmod 8$; it should be corrected in that case by replacing $\mathcal{F}_q$ by $\tilde{\mathcal{F}}_q$ as in (iv)(β) of Theorem 9.14.

9C. Local systems with infinite monodromy groups. Theorem 9.8 allows us to prove the following criterion for infinite monodromy.

Proposition 9.16. *Let $n \in \mathbb{Z}_{\geq 1}$, $q = 2^{2n+1}$, and consider the Airy sheaf $\mathcal{F}(q,f)$ defined in* (4.1.3) *with $q = 2^{2n+1}$, $f(x) \in \mathbb{F}_2[x]$, and $f(0) = 0$. Suppose that*

(i) *$2n+1$ is coprime to $|{}^2B_2(q)|$, and*
(ii) *there is some odd integer m coprime to $2n+1$ such that $|\mathrm{Trace}\big(\mathrm{Frob}_{0,\mathbb{F}_{2^m}}|\mathcal{F}(q,f)\big)| \neq 1$.*

Then $\mathcal{F}(q,f)$ has infinite geometric monodromy group.

Proof. Assume the contrary: $\mathcal{F}(q,f)$ has finite geometric monodromy group S. By Theorem 9.8, $S = {}^2B_2(q)$ and the arithmetic monodromy group of $\mathcal{F}(q,f)$ over $\mathbb{F}_2$ is $G = \mathbf{Z}(G) \times \mathrm{Aut}(S)$, where $\mathbf{Z}(G) \leq C_4$. In particular, $|G/S|$ divides $4(2n+1)$, and so S equals the arithmetic monodromy group of $\mathcal{F}(q,f)$ over $\mathbb{F}_{q^4}$. Moreover, $G = \langle g, S\rangle$ for the image g of $\mathrm{Frob}_{0,\mathbb{F}_2}$ in G, and we can write $g = zs$ with $z \in \mathbf{Z}(G)$, $s \in \mathrm{Aut}(S)$, and $\mathrm{Aut}(S) = \langle s, S\rangle$. Applying Corollary 9.5, we see that $|\mathrm{Trace}(g)| = |\mathrm{Trace}(s)| = 1$, a contradiction. □

Proposition 9.17. *Let $n \in \mathbb{Z}_{\geq 2}$, $q := 2^{2n+1}$, $r := [(n-1)/2]$, and define*

$$f_1(x) := \sum_{i=0}^{r} x^{1+2^{n-2i}}.$$

Consider the sheaf $\mathcal{F}(q,f)$ with $f(x) := f_1(x^{t(q)})$ as in (4.1.3). *Then for $m := 2[n/2]+1$ we have $|\mathrm{Trace}\big(\mathrm{Frob}_{0,\mathbb{F}_{2^m}}|\mathcal{F}(q,f)\big)| \neq 1$.*

Proof. As in the proof of Proposition 9.9, the starting point is that $\gcd(t(q), 2^m - 1) = 1$. To see this, note that $t(q) = q + 1 - 2q_0$ divides $q^4 - 1$, and $\gcd(q^4 - 1, 2^m - 1) = 2^{\gcd(4(2n+1),m)} - 1 = 1$. Thus for the field $k := \mathbb{F}_{2^m}$, the map $x \mapsto x^{t(q)}$ is bijective on k.

The sheaf $\mathcal{F}(q,f)$ was built out of the Witt vector $\big[x^{t(q)}, f_1(x^{t(q)})\big]$. Let us denote by $\mathcal{H}(q,f_1)$ the sheaf built by the same recipe, with same clearing factor, out of the Witt vector $[x, f_1(x)]$. Then we have

$$\mathrm{Trace}(\mathrm{Frob}_{0,k}|\mathcal{F}(q,f)) = \mathrm{Trace}(\mathrm{Frob}_{0,k}|\mathcal{H}(q,f_1)),$$

precisely because the map $x \mapsto x^{t(q)}$ is bijective on k.

Next, as in (9.9.2), we write the input vector $[x, f_1(x)]$ as $[x, xR(x)]$, with

$$R(x) := \sum_{i=0}^{r} x^{2^{n-2i}} = F^n(x) + F^{n-2}(x) + \ldots + F^{n-2r}(x),$$

and F denotes the absolute Frobenius. Now we can repeat the arguments in the proof of Proposition 9.9, and compute the form $\mathrm{Trace}_{k/\mathbb{F}_2}(\langle x,y\rangle)$ on $k \times k$ with $\langle x,y\rangle := xy + xR(y) + yR(x)$ as in (9.9.4). For any $x, y \in k$ we have $F^m(x) = x$, $F^m(y) = y$. If $2|n$, then $n = 2r+2$, $m = 2r+3$, and

$$\langle x,y\rangle = xy + y\big(\sum_{i=1}^{r+1} F^{2i}(x)\big) + \sum_{i=1}^{r+1} xF^{2i}(y)$$

has the same trace over $\mathbb{F}_2$ as of

$$xy + y\big(\sum_{i=1}^{r+1} F^{2i}(x)\big) + \sum_{i=1}^{r+1} F^{2r+3-2i}\big(xF^{2i}(y)\big) = xy + y\big(\sum_{i=1}^{r+1} F^{2i}(x)\big) + \sum_{i=1}^{r+1} yF^{2r+3-2i}(x)$$
$$= y\big(\sum_{j=0}^{2r+2} F^j(x)\big) = y\mathrm{Trace}_{k/\mathbb{F}_2}(x).$$

If $2 \nmid n$, then $n = m = 2r+1$, then

$$\langle x, y\rangle = xy + y\big(\sum_{i=0}^{r} F^{2i+1}(x)\big) + \sum_{i=0}^{r} xF^{2i+1}(y) = 3xy + y\big(\sum_{i=0}^{r-1} F^{2i+1}(x)\big) + \sum_{i=0}^{r-1} xF^{2i+1}(y)$$

has the same trace over $\mathbb{F}_2$ as of

$$xy + y\big(\sum_{i=0}^{r-1} F^{2i+1}(x)\big) + \sum_{i=0}^{r-1} F^{2r-2i}\big(xF^{2i+1}(y)\big) = xy + y\big(\sum_{i=0}^{r-1} F^{2i+1}(x)\big) + \sum_{i=0}^{r-1} yF^{2r-2i}(x)$$
$$= y\big(\sum_{j=0}^{2r} F^j(x)\big) = y\mathrm{Trace}_{k/\mathbb{F}_2}(x).$$

So in both cases, the symmetric bilinear form $\mathrm{Trace}_{k/\mathbb{F}_2}(\langle x, y\rangle)$ on $k \times k$ has kernel consisting of the elements $x \in k$ with $\mathrm{Trace}_{k/\mathbb{F}_2}(x) = 0$, that is, of exactly 2^{m-1} elements. Then the proof of Proposition 9.9 shows that $|\mathrm{Trace}\big(\mathrm{Frob}_{0,\mathbb{F}_{2^m}}|\mathcal{F}(q,f)\big)|$ is either 0 or $2^{(m-1)/2} > 1$, and hence can never be equal to 1 (since by hypothesis $n \geq 2$, and hence $m \geq 3$). □

Theorem 9.18. *Let $n \in \mathbb{Z}_{\geq 2}$, $q := 2^{2n+1}$, and consider the sheaf $\mathcal{F}(q,f)$ of rank $D := 2^n(2^{2n+1}-1)$, with $f(x) = f_1(x^{t(q)})$ and $f_1(x)$ as defined in Proposition 9.17. Assume in addition that $2n+1$ is coprime to $|{}^2B_2(q)|$; for instance, take $2n+1 = \ell^a$ for any odd prime $\ell \neq 5$ and any $a \in \mathbb{Z}_{\geq 1}$. Then the geometric monodromy group of $\mathcal{F}(q,f)$ is SL_D.*

Proof. We first apply Proposition 9.9, and note that m is coprime to $2(2n+1)$. It then follows from Proposition 9.16 that $\mathcal{F}(q,f)$ has infinite geometric monodromy group G_{geom}. By Theorem 8.4, $G_{\mathrm{geom}} = \mathrm{SL}_D$.

Suppose that $2n+1 = \ell^a$ for a prime ℓ, but ℓ divides $|{}^2B_2(q)|$. Then ℓ divides $q^4 - 1 = 2^{4\ell^a} - 1$. Since $\ell|(2^{\ell-1}-1)$, ℓ divides $\gcd(2^{4\ell^a}-1, 2^{\ell-1}-1) = 2^{\gcd(4\ell^a,\ell-1)} - 1$, and so ℓ divides $2^4 - 1 = 15$. But one knows that $3 \nmid |{}^2B_2(q)|$, so $r = 5$. □

More generally, to ensure that $2n+1$ is coprime to $|{}^2B_2(q)|$ for $q = 2^{2n+1}$, we can take any n such that $2n+1 = p_1^{a_1}p_2^{a_2}\dots p_t^{a_t}$, where $p_1 < p_2 < \dots < p_t$ are primes, $p_i \neq 5$, $a_i \in \mathbb{Z}_{\geq 1}$, and $p_i \nmid (p_j - 1)$ whenever $i < j$. Indeed, suppose p_j divides $|{}^2B_2(q)|$ for some j. Then p_j divides both $2^{p_j-1} - 1$ and $q^4 - 1 = 2^{4(2n+1)} - 1$. Since $\gcd(p_j - 1, 4(2n+1)) = \gcd(p_j - 1, 4\prod_{i=1}^t p_i^{a_i})$ divides 4, it follows that p_j divides $2^4 - 1 = 15$. But $p_j \neq 5$ by assumption, and $p_j \neq 3$ since $3 \nmid |{}^2B_2(q)|$, a contradiction.

References

[Abh] Abhyankar, S., Coverings of algebraic curves, *Amer. J. Math.* **79** (1957), 825–856.

[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.

[BCP] Bosma, W, Cannon, J., and Playoust, C., The Magma algebra system I: The user language. *J. Symbolic Comput.* **24** (1997), 235–265.

[Bo] Borel, A., Linear Algebraic Groups, Second enlarged edition, Graduate Texts in Mathematics, Springer-Verlag, 1991.

[Bur] Burkhardt, R., Die Zerlegungsmatrizen der Gruppen $PSL(2, p^f)$, *J. Algebra* **40** (1976), 75–96.

[C] Carter, R.W., Finite Groups of Lie type: Conjugacy Classes and Complex Characters, Wiley, Chichester, 1985.

[CR1] Curtis, C. W. and Reiner, I., Representation theory of finite groups and associative algebras, Interscience Publishers, New York 1962, xiv+689 pp.

[CR2] Curtis, C. W. and Reiner, I., Methods of representation theory – with applications to finite groups and orders, vol. I, Wiley & Sons, New York et al, 1981.

[Da] Dade, E., A new approach to Glauberman's correspondence, *J. Algebra* **270** (2003), 583–628.

[De1] Deligne, P., La conjecture de Weil II, *Publ. Math. I.H.E.S.* **52** (1981), 313–428.

[De2] Deligne, P., Les constantes des equations fonctionelles des fonctions L, (Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), pp. 501–597, Lecture Notes in Math., Vol. **349**, Springer, Berlin, 1973).

[Gr] Gross, B. H., Rigid local systems on $\mathbb{G}_m$ with finite monodromy, *Adv. Math.* **224** (2010), 2531–2543.

[GMPS] Guest, S., Morris J., Praeger, C. E., and Spiga, P., On the maximum orders of elements of finite almost simple groups and primitive permutation groups, *Trans. Amer. Math. Soc.* **367** (2015), 7665–7694.

[GLT] Guralnick, G.M., Larsen, M., and Tiep, P.H., Representation growth in positive characteristic and conjugacy classes of maximal subgroups, *Duke Math. J.* **161** (2012), 107–137.

[GT] Guralnick, R. M. and Tiep, P. H., The non-coprime $k(GV)$-problem, *J. Algebra* **293** (2005), 185–242.

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

[H] Humphreys, J.E., Introduction to Lie Algebras and Representation Theory, Springer, New York et al, 1972.

[Is1] Isaacs I. M., Characters of solvable and symplectic groups, *Amer. J. Math.* **95** (1973), 594– 635.

[Is2] Isaacs I. M., Glauberman correspondence Dade-method, preprint, July 2002.

[Is3] Isaacs, I.M., Character Theory of Finite Groups, AMS-Chelsea, Providence, 2006.

[Jan] Jantzen, J.C., Representations of Chevalley groups in their own characteristic, *Proc. Symp. Pure Math.* vol. **47** (1987), pt. 1, 127–146.

[KS] Kantor, W.M., and Seress, A., Large element orders and the characteristic of Lie-type simple groups, *J. Algebra* **322** (2009), 802–832.

[Ka1] Katz, N., Gauss sums, Kloosterman sums, and monodromy groups, Annals of Mathematics Studies, **116**. Princeton Univ. Press, Princeton, NJ, 1988. ix+246 pp.

[Ka2] Katz, N., Exponential sums and differential equations. Annals of Mathematics Studies, **124**, Princeton Univ. Press, Princeton, NJ, 1990. xii+430 pp.

[Ka4] Katz, N., From Clausen to Carlitz: low-dimensional spin groups and identities among character sums, *Mosc. Math. J.* **9** (2009), 57–89.

[Ka5] Katz, N., Exponential sums, Ree groups and Suzuki groups: conjectures, *Exp. Math.* **28** (2019), 49–56.

[KaS] 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.

[KRLT1] Katz, N., Rojas-León, A., and Tiep, P.H., A rigid local system with monodromy group the big Conway group $2.\mathsf{Co}_1$ and two others with monodromy group the Suzuki group $6.\mathsf{Suz}$, *Trans. Amer. Math. Soc.* **373** (2020), 2007–2044.

[KRLT2] Katz, N., Rojas-León, A., and Tiep, P.H., Rigid local systems and sporadic simple groups, *Mem. Amer. Math. Soc.* (to appear).

[KT1] Katz, N., and Tiep, P.H., Monodromy groups of Kloosterman and hypergeometric sheaves, *Geom. Funct. Analysis* **31** (2021), 562–662.

[KT2] Katz, N., and Tiep, P.H., Airy sheaves and generalized Airy sheaves, (in preparation).

[KlL] Kleidman, P. B., and Liebeck, M. W., The Subgroup Structure of the Finite Classical Groups, London Math. Soc. Lecture Note Ser. no. **129**, Cambridge University Press, 1990.

[Lu] Lübeck, F., Small degree representations of finite Chevalley groups in defining characteristic, *LMS J. Comput. Math.* **4** (2001), 135 − 169.

[Lun] Lüneburg, H., Ein einfacher Beweis für den Satz von Zsigmondy über primitive Primteiler von $A^n - 1$, in: Geometries and Groups, (edited by M. Aigner and D. Jungnickel), *Lect. Notes in Math.* **983**, 219–222, Springer Verlag, New York, 1981.

[MW] Manz, O, and Wolf, T. R., Representations of Solvable Groups, LMS Lecture Note Ser. no. **185**, Cambridge University Press, 1993.

[MNZ] Montgomery, H.L., Niven, I., and Zuckerman, H.S., An Introduction to Number Theory, fifth ed., Wiley & Sons, 1991.

[N1] Navarro, G., Fields, values and character extensions in finite groups, *J. Group Theory* **10** (2007), 279–285.

[N2] Navarro, G., Restriction of characters to Sylow normalizers, *Glasgow Math J.* **43** (2011), 311–315.

[OV] Onishchik, A.L., and Vinberg, E.B., Lie Groups and Algebraic Groups, Springer-Verlag, 1990.

[Pr] Premet, A.A., Weights of infinitesimally irreducible representations of Chevalley groups over a field of prime characteristic, *Math. USSR Sb.* **61** (1988), 167–183.

[Ro] Roitman, M., On Zsigmondy primes, *Proc. Amer. Math. Soc.* **125** (1997), 1913–1919.

[Se-Ta] Serre, J.-P., and Tate, J., Good reduction of abelian varieties, *Ann. of Math.* **88** (1968), 492–517.

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

[Suz] Suzuki, M., On a class of doubly transitive groups, *Annals of Math.* **75** (1962), 105–145.

[T] Tiep, P.H., Globally irreducible representations of the finite symplectic group $Sp_4(q)$, *Comm. Algebra* **22** (1994), 6439–6457.

[TZ] Tiep, P. H. and Zalesskii, A. E., Minimal characters of the finite classical groups, *Comm. Algebra* **24** (1996), 2093–2167.

[vG-vV] van der Geer, G., van der Vlugt, M., Reed-Muller codes and supersingular curves. I, *Compos. Math.* **84** (1992), 333–367.

[Tits] Tits, J., Algebraic and abstract simple groups, *Ann. of Math.* **80** (1964), 313–329

[Zs] Zsigmondy, K., Zur Theorie der Potenzreste, *Monatsh. Math. Phys.* **3** (1892), 265–284.

L. Alpöge, Department of Mathematics, Harvard University, Cambridge, MA 02138, U.S.A.
Email address: alpoge@math.harvard.edu

N.M. Katz, Department of Mathematics, Princeton University, Princeton, NJ 08544,U.S.A.
Email address: nmk@math.princeton.edu

G. Navarro, Departament de Matemàtiques, Universitat de València, 46100 Burjassot, València, Spain
Email address: gabriel@uv.es

E.A. O'Brien, University of Auckland, Auckland, New Zealand
Email address: e.obrien@auckland.ac.nz

P.H. Tiep, Department of Mathematics, Rutgers University, Piscataway, NJ 08854, U.S.A.
Email address: tiep@math.rutgers.edu