RIGID LOCAL SYSTEMS, MOMENTS, AND FINITE UNITARY GROUPS

NICHOLAS M. KATZ AND PHAM HUU TIEP

Contents

1. Introduction

For an **odd** integer $n \geq 3$, and a prime power $q \geq 3$, the irreducible representations (over $\mathbb{C}$) of lowest degree after the trivial representation of the group $\mathrm{SU}_n(q)$ are a symplectic representation of dimension $\frac{q^n+1}{q+1} - 1 = \frac{q^n-q}{q+1}$, and q representations of dimension $\frac{q^n+1}{q+1}$. When q is odd, exactly one of these q representations is orthogonal, otherwise none is. The direct sum of these $q+1$ representations is called the big Weil representation of $\mathrm{SU}_n(q)$.

In the paper [KT1], we wrote down $q+1$ rigid local systems on the affine line $\mathbb{A}^1/\overline{\mathbb{F}_p}$ whose geometric monodromy groups we conjectured to be the images of $\mathrm{SU}_n(q)$ in these $q+1$ representations. We were able to prove this only in the case when $n = 3$ and $\gcd(n, q+1) = 1$ (the condition that $\mathrm{SU}_n(q) = \mathrm{PSU}_n(q)$), where we made use of the results of Dick Gross [Gross]. In this paper, we use a completely different method, which starts[1] with results of Gross, to prove these conjectures for any odd $n \geq 3$ and for any odd prime power q, see Theorem 3.4.

The second author gratefully acknowledges the support of the NSF (grants DMS-1201374 and DMS-1665014). The paper is partially based upon work supported by the NSF under grant DMS-1440140 while the second author was in residence at the Mathematical Sciences Research Institute in Berkeley, California, during the Spring 2018 semester. It is a pleasure to thank the Institute for support, hospitality, and stimulating environments.

[1]The results here use the results of [KT2], which in turn uses the resuts of [KT1] for SL_2, and those use [Gross] in an essential way.

The method used here, which requires that q be odd, is based on a striking group-theoretic relation between the Weil representations of $\mathrm{SU}_n(q)$ and $\mathrm{Sp}_{2n}(q)$, and on the determination of those subgroups of $\mathrm{Sp}_{2n}(q)$ to which the Weil representation restricts "as though" it were the Weil representation of $\mathrm{SU}_n(q)$, cf. Theorem 2.3. We are able to apply this result to our local systems, in Section 3, by invoking results of [KT2], which was devoted to questions around $\mathrm{Sp}_{2n}(q)$. Furthermore, our Theorem 3.3 also improves the main results Theorems 1.1 and 4.8 of [KT2] in the case $2 \nmid n$, by removing the condition that $p \nmid n \cdot \log_p(q)$ for the prime $p|q$.

In the course of thinking about these questions, we stumbled upon a very striking representation-theoretic fact about the q irreducible representations of $\mathrm{SU}_n(q)$ ($n \geq 3$ odd, q odd) of dimension $\frac{q^n+1}{q+1}$. For each of them, their n^{th} moment (i.e. the dimension of the space of invariants in the n^{th} tensor power of the representation in question) is one, cf. Theorem 4.11. For the irreducible repesentation of dimension $\frac{q^n+1}{q+1} - 1$, the n^{th} moment vanishes. At present we do not have a conceptual explanation for this.

Given this result about n^{th} moments for $\mathrm{SU}_n(q)$ when n is odd, it is natural to wonder about the situation for n^{th} moments when n is even. [For n even and $q \geq 3$ a prime power, the irreducible representations (over $\mathbb{C}$) of lowest degree after the trivial representation of the group $\mathrm{SU}_n(q)$ are an orthogonal representation of dimension $\frac{q^n-1}{q+1} + 1 = \frac{q^n+q}{q+1}$, and q representations of dimension $\frac{q^n-1}{q+1}$.] Already for $n = 4$, the result is not so nice, cf. Theorem 5.1.

2. Unitary-type subgroups of finite symplectic groups

Let $q = p^f$ be any prime power and $n \geq 2$. It is well known, see e.g. [TZ2, §4], that the function

$$\zeta_{n,q} = \zeta_n : g \mapsto (-1)^n (-q)^{\dim_{\mathbb{F}_{q^2}} \mathrm{Ker}(g - 1_W)}$$

defines a complex character, called the (reducible) *Weil character*, of the general unitary group $\mathrm{GU}_n(q) = \mathrm{GU}(W)$, where $W = \mathbb{F}_{q^2}^n$ is a non-degenerate Hermitian space with Hermitian product $\circ$. Note that the $\mathbb{F}_q$-bilinear form

$$(u|v) = \mathrm{Trace}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\theta u \circ u)$$

on W, for a fixed $\theta \in \mathbb{F}_{q^2}^\times$ with $\theta^{q-1} = -1$, is non-degenerate symplectic. This leads to an embedding

$$\tilde{G} := \mathrm{GU}_n(q) \hookrightarrow \mathrm{Sp}_{2n}(q).$$

Moreover, if q is odd then the restriction of any of the two big Weil characters (of degree q^n, and denoted $\mathsf{Weil}_{1,2}$ in [KT2]) of $\mathrm{Sp}_{2n}(q)$ to $\mathrm{GU}_n(q)$ is exactly the big Weil character ζ_n, cf. [TZ2, §4]. We will also denote by ζ_n the restriction of this character to the special unitary group $G := \mathrm{SU}_n(q)$.

Fix a generator σ of $\mathbb{F}_{q^2}^\times$ and set $\rho := \sigma^{q-1}$. We also fix a primitive $(q^2-1)^{\text{th}}$ root of unity $\boldsymbol{\sigma} \in \mathbb{C}^\times$ and let $\boldsymbol{\rho} = \boldsymbol{\sigma}^{q-1}$. Then

$$(\mathsf{Weil}_1)|_{\tilde{G}} = \zeta_n = \sum_{i=0}^{q} \tilde{\zeta}_{i,n} \tag{2.0.1}$$

decomposes as the sum of $q+1$ characters of $\tilde{G}$, where

$$\tilde{\zeta}_{i,n}(g) = \frac{(-1)^n}{q+1} \sum_{l=0}^{q} \boldsymbol{\rho}^{il}(-q)^{\dim \operatorname{Ker}(g - \rho^l \cdot 1_W)}; \tag{2.0.2}$$

see [TZ2, Lemma 4.1]. In particular, $\tilde{\zeta}_{i,n}$ has degree $(q^n-(-1)^n)/(q+1)$ if $i>0$ and $(q^n+(-1)^n q)/(q+1)$ if $i=0$.

We will let $\zeta_{i,n}$ denote the restriction of $\tilde{\zeta}_{i,n}$ to $G = \mathrm{SU}_n(q)$, for $0 \le i \le q$. If $n \ge 3$, then these $q+1$ characters are all irreducible and distinct. If $n=2$, then $\zeta_{i,n}$ is irreducible, unless q is odd and $i=(q+1)/2$, in which case it is a sum of two irreducible characters of degree $(q-1)/2$, see [TZ2, Lemma 4.7]. Formula (2.0.2) implies that Weil characters $\zeta_{i,n}$ enjoy the following branching rule while restricting to the natural subgroup $H := \mathrm{Stab}_G(w) \cong \mathrm{SU}_{n-1}(q)$ ($w \in W$ any anisotropic vector):

$$\zeta_{i,n}|_H = \sum_{j=0,\ j\neq i}^{q} \zeta_{j,n-1}. \tag{2.0.3}$$

Furthermore, the complex conjugation fixes $\tilde{\zeta}_{0,n}$ and sends $\tilde{\zeta}_{j,n}$ to $\tilde{\zeta}_{q+1-j,n}$ when $1 \le j \le q$. As $n \ge 3$ is odd, it is also known that $\tilde{\zeta}_{0,n}$ is of symplectic type; let $\Psi_0 : \tilde{G} \to \mathrm{Sp}(V)$ be a complex representation affording this character. If $2 \nmid q$, then $\tilde{\zeta}_{(q+1)/2,n}$ is of orthogonal type; let $\Psi_{(q+1)/2} : \tilde{G} \to \mathrm{O}(V)$ be a complex representation affording this character. In the remaining cases, let $\Psi_i : \tilde{G} \to \mathrm{GL}(V)$ be a complex representation affording the character $\tilde{\zeta}_{i,n}$.

Lemma 2.1. *Assume $n \ge 3$ is odd and $(n,q) \neq (3,2)$.*

- (i) $\Psi_0(\mathrm{GU}_n(q)) \cong \mathrm{PGU}_n(q)$ *is contained in* $\mathrm{Sp}(V)$ *and contains* $\Psi_0(\mathrm{SU}_n(q))$ *with index* $d := \gcd(n, q+1)$.
- (ii) *If* $1 \le i \le q$, *then* $\mathrm{Ker}(\Psi_i)$ *is a central subgroup of order* $\gcd(i, q+1)$, *and* $\mathrm{Ker}(\Psi_i|_{\mathrm{SU}_n(q)})$ *is a central subgroup of order* $\gcd(i, n, q+1)$.
- (iii) *If* $2 \nmid q$, *then* $\Psi_{(q+1)/2}(\mathrm{GU}_n(q)) \cap \mathrm{SO}(V)$ *contains* $\Psi_{(q+1)/2}(\mathrm{SU}_n(q))$ *with index* $(q+1)/2$.
- (iv) *If* $1 \le i \le q$ *and* $i \neq (q+1)/2$, *then* $\Psi_i(\mathrm{GU}_n(q)) \cap \mathrm{SL}(V)$ *contains* $\Psi_i(\mathrm{SU}_n(q))$ *with index* $\gcd(i, q+1)$.

Proof. According to [TZ2, §4], one can label Ψ_i in such a way that

$$\Psi_i(z) = \boldsymbol{\rho}^i \cdot 1_V$$

for the generator $z = \rho \cdot 1_W$ of $\mathbf{Z}(\tilde{G}) \cong C_{q+1}$. In particular, $z \in \mathrm{Ker}(\Psi_0)$, and (i) follows.

Now we can assume $1 \leq i \leq q$. Then $z^j \in \mathrm{Ker}(\Psi_i)$ if and only if j is divisible by $(q+1)/\gcd(i, q+1)$. Furthermore, $z^{j(q+1)/d} \in \mathrm{Ker}(\Psi_i|_{\mathrm{SU}_n(q)})$ if and only if j is divisible by $d/\gcd(i,d) = d/\gcd(i,n,q+1)$ for $d := \gcd(n, q+1)$, equivalently, if $j(q+1)/d$ is divisible by $(q+1)/\gcd(i,n,q+1)$. Hence (ii) follows.

Consider the element $g := \mathrm{diag}(\rho, 1, 1, \ldots, 1) \in \tilde{G}$; note that $\tilde{G} = \langle G, g \rangle$. Then (2.0.2) implies that

$$\tilde{\zeta}_{i,n}(g^k) = -\frac{q^{n-1} - (-1)^{n-1}}{q+1} + (-1)^{n-1}\boldsymbol{\rho}^{ik}$$

when $1 \leq k \leq q$. It follows that $\Psi_i(g)$ has eigenvalues $\boldsymbol{\rho}^j$, $1 \leq j \leq q$, with multiplicity $(q^{n-1}-1)/(q+1)$ if $k \neq i$ and $1 + (q^{n-1}-1)/(q+1)$ if $k = i$, and so

$$\det(\Psi_i(g)) = \boldsymbol{\rho}^i.$$

Since $\mathrm{SU}_n(q)$ is perfect, (ii) and (iii) follow. □

We will now show that, when $n \geq 3$ is odd and q is odd, the splitting (2.0.1) of a big Weil character Weil_i of $\mathrm{Sp}_{2n}(q)$ on its restriction to $\mathrm{SU}_n(q)$ into a sum of $q+1$ irreducible constituents of prescribed degrees characterizes $\mathrm{SU}_n(q)$ uniquely (up to conjugacy).

Recall [Zs] that if $a \geq 2$ and $n \geq 2$ are any integers with $(a,n) \neq (2,6)$, $(2^k-1, 2)$, then $a^n - 1$ has a *primitive prime divisor*, that is, a prime divisor ℓ that does not divide $\prod_{i=1}^{n-1}(a^i - 1)$; write $\ell = \mathrm{ppd}(a,n)$ in this case. Furthermore, if in addition $a, n \geq 3$ and $(a,n) \neq (3,4)$, $(3,6)$, $(5,6)$, then $a^n - 1$ admits a *large primitive prime divisor*, i.e. a primitive prime divisor ℓ where either $\ell > m+1$ (whence $\ell \geq 2m+1$), or $\ell^2 | (a^m - 1)$, see [F2].

We will need the following recognition theorem [KT2, Theorem 2.6], which was obtained relying on [GPPS].

Theorem 2.2. *Let $q = p^f$ be a power of an odd prime p and let $d \geq 2$. If $d = 2$, suppose that $p^{df} - 1$ admits a primitive prime divisor $\ell > 5$. If $d \geq 3$, suppose in addition that $(p, df) \neq (3,4)$, $(3,6)$, $(5,6)$, so that $p^{df} - 1$ admits a large primitive prime divisor ℓ, in which case we choose such an ℓ to maximize the ℓ-part of $p^{df} - 1$. Let $W = \mathbb{F}_q^d$ and let G be a subgroup of $\mathrm{GL}(W) \cong \mathrm{GL}_d(q)$ of order divisible by the ℓ-part $Q := (q^d - 1)_\ell$ of $q^d - 1$. Then either $L := \mathbf{O}^{\ell'}(G)$ is a cyclic ℓ-group of order Q, or there is a divisor $j < d$ of d such that one of the following statements holds.*

(i) *$L = \mathrm{SL}(W_j) \cong \mathrm{SL}_{d/j}(q^j)$, $d/j \geq 3$, and W_j is W viewed as a d/j-dimensional vector space over $\mathbb{F}_{q^j}$.*
(ii) *$2j | d$, W_j is W viewed as a d/j-dimensional vector space over $\mathbb{F}_{q^j}$ endowed with a non-degenerate symplectic form, and $L = \mathrm{Sp}(W_j) \cong \mathrm{Sp}_{d/j}(q^j)$.*

(iii) $2|jf$, $2 \nmid d/j$, W_j *is* W *viewed as a* d/j*-dimensional vector space over* $\mathbb{F}_{q^j}$ *endowed with a non-degenerate Hermitian form, and* $L = \mathrm{SU}(W_j) \cong \mathrm{SU}_{d/j}(q^{j/2})$.

(iv) $2j|d$, $d/j \geq 4$, W_j *is* W *viewed as a* d/j*-dimensional vector space over* $\mathbb{F}_{q^j}$ *endowed with a non-degenerate quadratic form of type* $-$, *and* $L = \Omega(W_j) \cong \Omega^-_{d/j}(q^j)$.

(v) $(p, df, L/\mathbf{Z}(L)) = (3, 18, \mathrm{PSL}_2(37))$, $(17, 6, \mathrm{PSL}_2(13))$.

The main result of this section is the following theorem:

Theorem 2.3. *Let* $q = p^f$ *be a power of an odd prime* p *and let* $n \geq 3$ *be an odd integer. Let* $W = \mathbb{F}_q^{2n}$ *be a non-degenerate symplectic space, and* $H := \mathrm{Sp}(W) \cong \mathrm{Sp}_{2n}(q)$, *and let* Φ *be a complex Weil representation* Weil_i *of* H *of degree* q^n *as in* [KT2, §1]. *Suppose that* $G \leq H$ *is a subgroup such that* $\Phi|_G = \oplus_{j=0}^q$ *is a sum of* $q+1$ *irreducible summands,* Φ_0 *of degree* $(q^n - q)/(q+1)$ *and* Φ_j *of degree* $(q^n+1)/(q+1)$ *for* $1 \leq j \leq q$. *Then* W *can be viewed as an* n*-dimensional vector space over* $\mathbb{F}_{q^2}$ *endowed with a* G*-invariant non-degenerate Hermitian form such that*

$$\mathrm{SU}_n(q) \cong \mathrm{SU}(W) \lhd G \leq \mathrm{GU}(W) \cong \mathrm{GU}_n(q).$$

Proof. (a) First we assume that $(n, q) \neq (3, 3)$ and $(3, 5)$; in particular, so that $p^{2nf} - 1$ admits a large primitive prime divisor ℓ, in which case we choose such an ℓ to maximize the ℓ-part of $p^{2nf} - 1$. Note the assumptions imply that $|G|$ is divisible by both $(q^n - q)/(q + 1)$ and $(q^n + 1)/(q + 1)$. In particular, $G < \mathrm{GL}(W)$ has order divisible by

$$qQ := q(p^{2nf} - 1)_\ell. \tag{2.3.1}$$

Let $L := \mathbf{O}^{\ell'}(G)$ and $d(L)$ denote the smallest degree of nontrivial complex irreducible characters of L. Note that

$$d(L) \leq (q^n + 1)/(q + 1) \leq (q^n + 1)/4. \tag{2.3.2}$$

(Otherwise $L \leq \mathrm{Ker}(\Phi_1)$, whence Φ_1 could be viewed as an irreducible representation of G/L and so would have been of ℓ'-degree.) Furthermore, if L is cyclic of order Q, then by Ito's theorem, the degree of any irreducible character of G divides $|G/L|$, an integer coprime to ℓ, and so again G cannot be irreducible on Φ_1. Now we can apply Theorem 2.2 to arrive at one of the following cases.

(i) $L \cong \mathrm{SL}_{2n/j}(q^j)$ for some divisor $1 \leq j \leq n$ of $2n$. In this case, if $j \leq 2n/3$ then by [TZ1, Theorem 3.1] we have

$$d(L) > q^{j(2n/j)-1} = q^{2n-2n/j} > q^n,$$

contradicting (2.3.2). If $j = n$, then $q^j = q^n \geq 27$ and so

$$d(L) \geq (q^n - 1)/2 > (q^n + 1)/4,$$

again contradicting (2.3.2).

(ii) $L \cong \mathrm{Sp}_{2n/j}(q^j)$ for some divisor $1 \leq j < n/2$ of n. Then by [TZ1, Theorem 1.1] we have

$$d(L) > (q^n - 1)/2 > (q^n + 1)/4,$$

contradicting (2.3.2).

(iii) There is some even divisor $j = 2k$ of $2n$ with $k|n$ and $2 \nmid n/k > 1$, such that W can be viewed as a $2n/j$-dimensional vector space over $\mathbb{F}_{q^j}$ endowed with a non-degenerate Hermitian form and $L = \mathrm{SU}(W) \cong \mathrm{SU}_{n/k}(q^k)$. Suppose first that $k > 1$, and let ψ be an irreducible constituent of the L-character afforded by Φ_0, so that $\psi(1) < (q^n + 1)/4$. By [TZ1, Theorem 4.1],

$$\psi(1) \in \left\{1, \frac{q^n + 1}{q^k + 1}, \frac{q^n - q^k}{q^k + 1}\right\}.$$

The proof of (2.3.2) rules out the possibility $\psi(1) = 1$. Next,

$$\psi(1) | \dim \Phi_0 = (q^n - q)/(q + 1)$$

by Clifford's theorem, implying $\psi(1) \neq (q^n - q^k)/(q^k + 1)$. The remaining possibility $\psi(1) = (q^n + 1)/(q^k + 1)$ is also ruled out since $\ell \nmid \dim \Phi_0$. We have shown that $k = 1$, i.e. $L = \mathrm{SU}(W) \cong \mathrm{SU}_n(q)$. This implies that

$$L \lhd G \leq \mathbf{N}_{\mathrm{Sp}(W)}(L) = \mathrm{GU}(W) \rtimes \langle \sigma \rangle \cong \mathrm{GU}_n(q) \rtimes C_2.$$

Here, σ is an involutive automorphism of $\mathrm{GU}(W)$ that acts as inversion on

$$\langle z \rangle = \mathbf{Z}(\mathrm{GU}(W)) \cong C_{q+1}. \tag{2.3.3}$$

Recall the decomposition

$$\Phi|_{\mathrm{GU}(W)} = \oplus_{i=0}^{q} \Psi_i, \tag{2.3.4}$$

with Ψ_0 of degree $(q^n - q)/(q + 1)$ and Ψ_i of degree $(q^n + 1)/(q + 1)$ for $1 \leq i \leq q$, see the discussion preceding Lemma 2.1. In fact, one can find a primitive $(q + 1)^{\text{th}}$ root of unity $\xi \in \mathbb{C}^\times$ such that $\Psi_i(z)$ is the multiplication by ξ^i. In particular, σ fuses Ψ_1 and Ψ_q. The assumption on $\Phi|_G$ now implies that $G \leq \mathrm{GU}(W)$, as stated.

(iv) $L \cong \Omega^-_{2n/j}(q^j)$ for some divisor $1 \leq j < n/2$ of the odd integer n. If $j \leq n/5$, then by [TZ1, Theorem 1.1] we have

$$d(L) > q^n + 1,$$

contradicting (2.3.2). If $j = n/3$, then L is a quasisimple quotient of $\mathrm{PSU}_4(q^{n/3})$ with $q^{n/3} > 5$, and so by [TZ1, Theorem 1.1] we have

$$d(L) = \frac{q^{4n/3} - 1}{q^{n/3} + 1} > q^n/2,$$

again contradicting (2.3.2).

(v) $(p, nf, L/\mathbf{Z}(L)) = (3, 9, \mathrm{PSL}_2(37))$. Note that the smallest dimension of a nontrivial irreducible representation of L over $\overline{\mathbb{F}}_3$ is 18 (see e.g. [TZ1, Table I]), so

$(q,n) = (3,9)$ and $L = \mathrm{SL}_2(37)$ acts absolutely irreducibly on $W = \mathbb{F}_3^{18}$. This in turn implies that

$$\mathbf{C}_{\mathrm{Sp}(W)}(L) = \mathbf{Z}(L) = C_2,$$

and so $L \lhd G \leq \mathbf{N}_{\mathrm{Sp}(W)}(L) \leq L \cdot C_2$. But in this case, G cannot have an irreducible complex representation of degree

$$\dim \Phi_1 = (q^n+1)/(q+1) = (3^9+1)/4.$$

(vi) $(p, nf, L/\mathbf{Z}(L)) = (17, 6, \mathrm{PSL}_2(13))$. In this case $(q,n) = (17,3)$ and $L = \mathrm{SL}_2(13)$ acts absolutely irreducibly on $W = \mathbb{F}_{17}^6$. As in (v), this implies that

$$\mathbf{C}_{\mathrm{Sp}(W)}(L) = \mathbf{Z}(L) = C_2,$$

and $L \lhd G \leq \mathbf{N}_{\mathrm{Sp}(W)}(L) \leq L \cdot C_2$, whence G cannot have an irreducible complex representation of degree

$$\dim \Phi_1 = (q^n+1)/(q+1) = (17^3+1)/18.$$

(b) It remains to consider the two cases $(n,q) = (3,3)$ and $(3,5)$. Let M be a maximal subgroup of $\mathrm{Sp}(W)$ that contains G. Then condition (2.3.1) also holds for $|M|$; furthermore, the maximal degree of complex irreducible characters of M must be at least $(q^n+1)/(q+1) = 7$, respectively 21, since $\Phi_1 \in \mathrm{Irr}(G)$. First suppose that $q = 5$. Then, according to Tables 8.27 and 8.28 of [BHR], one of the following possibilities occurs.

• $M = 2J_2$. In this case, since $|G|$ is divisible by $3 \cdot 5 \cdot 7$, see (2.3.1), we see by inspecting maximal subgroups of J_2 [Atlas] that $G = M$. But then G does not admit any complex irreducible representation of degree $\dim \Phi_0 = 20$.

• $M = \mathrm{SL}_2(125) \rtimes C_3$. In this case, since $|G \cap [M,M]|$ is divisible by $5 \cdot 7$, see (2.3.1), we see by inspecting maximal subgroups of $\mathrm{PSL}_2(125)$ [BHR, Table 8.1] that $G \rhd \mathrm{SL}_2(125)$. But then $d(G) \geq 62$ (see e.g. [TZ1, Table I]), violating (2.3.2).

• $M = \mathrm{GU}_3(5) \rtimes C_2$. If $G \geq N := \mathrm{SU}_3(5)$, then we can argue as in (iii) above. Suppose $G \not\geq N$. Since $L := G \cap N \lhd G$ has order divisible by $5 \cdot 7$, see (2.3.1), we see by inspecting maximal subgroups of $\mathrm{PSL}_3(5)$ and Alt_7 [Atlas] that $L = 3\mathrm{Alt}_7$, and $\mathbf{Z}(L) = \langle z^2 \rangle$ with $\langle z \rangle = \mathbf{Z}(\mathrm{GU}_3(5))$ as defined in (2.3.3). Using the decomposition (2.3.4), we may assume that $\Phi_i = (\Psi_i)|_G$ for $0 \leq i \leq q$. As mentioned in (iii), the subgroup C_2 fuses Ψ_1 with Ψ_5, hence Φ_1 with Φ_5. Thus $G \leq \mathrm{GU}_3(5)$, and so $|G/L|$ and $|\mathbf{N}_{\mathrm{GU}_3(5)}(L)/L|$ both divide 6. Note that $\mathbf{N}_{\mathrm{GU}_3(5)}(L)$ contains the central involution of $\mathrm{GU}_3(5)$ which lies outside of $\mathrm{SU}_3(5)$. It follows that G induces a subgroup X of outer automorphisms of L of order dividing 3, whence $X = 1$ as $|\mathrm{Out}(\mathrm{Alt}_7)| = 2$ [Atlas]. Now let $g \in L$ be of order 7. Then $\Phi_0(g) = \Psi_0(g)$ has trace -1. On the other hand, as G induces only inner automorphisms on L, we see that $(\Phi_0)|_L$ must be a direct sum of two copies of a single irreducible complex representation Φ' (of dimension 10) of L and we arrive at the contradiction that $\Phi'(g)$ has trace $-1/2$.

(c) Finally, we consider the case $q = 3$. Inspecting the list of maximal subgroups of $\mathrm{PSp}_6(3)$ in [Atlas], we arrive at the following possibilities for M. By (2.3.1), G contains an element $g \in G$ of order 7. According to [Atlas], we may assume that $\Phi_0 \oplus \Phi_2 = \Lambda|_G$, where Λ is an irreducible Weil representation of degree 13 of $\mathrm{Sp}_6(3)$ and contains the central involution t of $\mathrm{Sp}_6(3)$ in its kernel, and that $\Lambda(g)$ has trace -1.

• $M = \mathrm{SL}_2(13)$. In this case, since $|G|$ is divisible by $3 \cdot 7$, see (2.3.1), we see by inspecting maximal subgroups of $\mathrm{PSL}_2(13)$ [Atlas] that $G = M$. Note that t is the central involution of G. Now the conditions that $t \in \mathrm{Ker}(\Lambda)$ and $\Lambda(g)$ has trace -1 imply by [Atlas] that $\Lambda|_G$ is irreducible, a contradiction.

• $M = \mathrm{SL}_2(27) \cdot 3$. In this case, since $|G|$ is divisible by 7, we see by inspecting maximal subgroups of $\mathrm{PSL}_2(27)$ [Atlas] that either $G \geq [M, M] = \mathrm{SL}_2(27)$ or $G \cap [M, M]$ is contained in a dihedral group D_{28}. It is easy to see that in the former case $d(G) \geq 13$ contradicting (2.3.2), and in the latter case G does not admit any complex irreducible representation of dimension $\dim \Phi_1 = 7$.

• $M = \mathrm{GU}_3(3) \rtimes C_2$. If $G \geq N := \mathrm{SU}_3(3)$, then we can argue as in (iii) above. Suppose $G \not\geq N$. Since $L := G \cap N \lhd G$ has order divisible by $3 \cdot 7$, see (2.3.1), we see by inspecting maximal subgroups of $\mathrm{SU}_3(3)$ and $\mathrm{PSL}_2(7)$ [Atlas] that either L is of order 21 or $L = \mathrm{PSL}_2(7)$. The former case is ruled out since $(\Phi_1)|_L$ is irreducible of dimension 7. In the latter case, fix an involution $s \in L$. We may assume that

$$(\Phi_i)|_L = (\Psi_i)|_L$$

for the representations Ψ_i defined in (2.3.4), and furthermore Ψ_2 is self-dual of dimension 7. Using [Atlas] we see that $\Psi_1(s)$ has trace 3 and $\Psi_1(g)$ has trace 0, whence $(\Phi_1)|_L = (\Psi_1)|_L$ is the sum of two irreducible representations of dimensions 1 and 6, contradicting the irreducibility of Φ_1 on $G \rhd L$. □

In the next statement, we consider a non-degenerate symplectic space $W = \mathbb{F}_p^{2N}$, a (reducible) big Weil representation of degree q^N of $G = \mathrm{Sp}(W) \cong \mathrm{Sp}_{2N}(p)$ with character ω as in [KT2]; in particular,

$$|\omega(g)| = |\mathbf{C}_W(g)|^{1/2} \tag{2.3.5}$$

for any $g \in G$. Let $N = AB$ and $B = bj$ for some positive integers A, B, b, j. We may then assume that W is obtained from the symplectic space $W_1 := \mathbb{F}_{p^B}^{2A}$ (with a Witt basis $(e_1, \ldots, e_A, f_1, \ldots, f_A)$) by base change from $\mathbb{F}_{p^B}$ to $\mathbb{F}_p$. Using this basis we can consider the transformation

$$\sigma : \sum_{i=1}^{A} (x_i e_i + y_i f_i) \mapsto \sum_{i=1}^{A} (x_i^r e_i + y_i^r f_i)$$

induced by the Galois automorphism $x \mapsto x^r$ for $r := p^j$. Then, as in [KT2, §2] we can consider the standard subgroup

$$H = \mathrm{Sp}(2A, p^B) \rtimes C_b$$

of G, where $C_b = \langle \sigma \rangle$.

Theorem 2.4. *Each value $|\omega(x)|^2$, $x \in H$, is a power of $r = p^j$. Furthermore, there is some $h \in H$ such that $|\omega(h)|^2 = r$.*

Proof. Note that H embeds in $\mathrm{Sp}(2Ab, p^j)$, and so the first statement follows by applying (2.3.5) to a big Weil representation of $\mathrm{Sp}(2Ab, p^j)$. To define h, consider the $\mathbb{F}_r$-linear map

$$f : \mathbb{F}_{p^B} \to \mathbb{F}_{p^B}, \ x \mapsto x - x^r.$$

Viewed as a vector space over $\mathbb{F}_r$, $\mathrm{Ker}(f)$ has dimension 1. Hence f cannot be surjective, and so we can find

$$\alpha \in \mathbb{F}_{p^B} \smallsetminus \mathrm{Im}(f).$$

Let J denote the Jordan block of size $A \times A$ with eigenvalue α^{-1}, and let $g \in H$ have the following matrix

$$\begin{pmatrix} {}^t(\alpha J)^{-1} & \alpha^2 J \\ 0 & \alpha J \end{pmatrix}$$

in the chosen basis $(e_1, \ldots, e_A, f_1, \ldots, f_A)$ of W_1. We will show that $h = g\sigma$ satisfies $|\omega(h)|^2 = r$. According to (2.3.5), it suffices to show that h fixes exactly r vectors in W_1. To this end, suppose that $w = \sum_{i=1}^{A}(x_i e_i + y_i f_i)$ is fixed by h, where $x_i, y_i \in \mathbb{F}_{p^B}$. Comparing the coefficient for f_A we have

$$y_A^r = y_A$$

implying $y_A \in \mathbb{F}_r$. Next, comparing the coefficient for f_{A-1} we see that

$$y_{A-1}^r + \alpha y_A^r = y_{A-1},$$

and so $\alpha y_A = f(y_{A-1})$. Continuing in the same fashion, we conclude that

$$y_1 \in \mathbb{F}_r, \ y_2 = y_3 = \ldots = y_A.$$

Thus we have shown that $v := \sum_{i=1}^{A} y_i f_i = y_1 f_1$. Letting $u := w - v = \sum_{i=1}^{A} x_i e_i$, we have

$${}^t(\alpha J)^{-1}\sigma(u) + \alpha^2 J \sigma(v) = u,$$

i.e.

$$\sigma(u) + {}^t(\alpha J)\alpha^2 J \sigma(v) = {}^t(\alpha J)(u).$$

Comparing the coefficient for e_1, we get

$$x_1^r + \alpha y_1 = x_1,$$

and so $\alpha y_1 = f(x_1)$. Again by the choice of α, we must have that $y_1 = 0$ and $x_1 \in \mathbb{F}_r$. Next, comparing the coefficient for e_2, we get

$$x_2^r = \alpha x_1 + x_2,$$

and so $-\alpha x_1 = f(x_2)$. By the choice of α, we must have that $x_1 = 0$ and $x_2 \in \mathbb{F}_r$. Continuing in the same fashion, we conclude that

$$x_A \in \mathbb{F}_r,\ x_1 = x_2 = \ldots = x_{A-1}.$$

Thus $w = x_A e_A$ with $x_A \in \mathbb{F}_r$. □

Lemma 2.5. *Let $q = p^f \geq 3$ be a prime power and let A, B, b, c be positive integers, and let $H = \mathrm{Sp}_{2A}(p^B) \rtimes C_b$ as above. Then the following statements hold.*

(i) *If $c \geq 3$, then $\mathrm{SU}_{Ac}(q)$ cannot embed in H.*

(ii) *Assume in addition that $(p, A, B) \neq (3, 1, 1)$. Then the only quotient groups of H are H, $H/\mathbf{Z}(H) = \mathrm{PSp}_{2A}(p^B) \rtimes C_b$, and quotients of C_b.*

Proof. (i) Assume the contrary. Since $c, q \geq 3$, $\mathrm{SU}_{Ac}(q)$ is perfect, and so it embeds in $\mathrm{Sp}_{2A}(p^B) < \mathrm{Sp}_{2A}(\overline{\mathbb{F}}_p)$. In particular, $\mathrm{SU}_{Ac}(q)$ has a nontrivial absolutely irreducible representation in characteristic p of dimension $\leq 2A \leq Ac - 1$. But this contradicts [KlL, Proposition 5.4.11].

(ii) The assumption on (p, A, B) ensures that $L := [H, H] = \mathrm{Sp}_{2A}(p^B)$ is quasisimple, with $S = L/\mathbf{Z}(H) \cong \mathrm{PSp}_{2A}(p^B)$ being simple. Furthermore, $H/\mathbf{Z}(H)$ acts faithfully on S.

Suppose that $N \lhd H$. If $N \geq L$, then H/N is a quotient of $H/L \cong C_b$. In the remaining case, we have that $N \cap L$ is a proper normal subgroup of L, and so contained in $\mathbf{Z}(H)$. In particular, $[N, L] \leq N \cap L$ centralizes L, i.e. $[[N, L], L] = 1$. Since $L = [L, L]$, the Three Subgroups Lemma implies that $[N, L] = 1$, whence

$$N \leq \mathbf{C}_H(L) \leq \mathbf{C}_H(S) = \mathbf{Z}(H).$$

Thus either $N = 1$ or $N = \mathbf{Z}(H)$. □

3. Local systems and Weil representations

In this section, we fix an odd prime p, and a prime $\ell \neq p$, so that we can avail ourselves of $\overline{\mathbb{Q}_\ell}$-adic cohomology. We also fix a nontrivial additive character ψ of $\mathbb{F}_p$. We denote by χ_2 the quadratic character of $\mathbb{F}_p^\times$, and we define

$$A := A_{\mathbb{F}_p} := -\sum_{x \in \mathbb{F}_p^\times} \psi(-2x)\chi_2(x).$$

For $k/\mathbb{F}_p$ a finite extension, we define

$$A_k := A^{\deg(k/\mathbb{F}_p)}.$$

We denote by ψ_k the additive character of k given by

$$\psi_k := \psi \circ \mathrm{Trace}_{k/\mathbb{F}_p}.$$

In [KT2, Section 1], we introduced, for each integer $n \geq 2$ and each power $q = p^a$ of the odd prime p, the local system

$$\mathcal{W}(\psi, n, q)$$

on $\mathbb{A}^2/\mathbb{F}_p$ whose trace function at a point $(s,t) \in \mathbb{A}^2(k)$, k a finite extension of $\mathbb{F}_p$, is the sum

$$(-1/A_k) \sum_{x \in k} \psi_k(x^{q^n+1} + sx^{q+1} + tx^2).$$

We proved there [KT2, Theorem 1.1, 4.8] that when both n and $a := \log_p(q)$ are prime to p, the geometric monodromy group G_{geom} of $\mathcal{W}(\psi, n, q)$ was $\mathrm{Sp}_{2n}(q)$ in one of its big Weil representations (of degree q^n), and that after extension of scalars from $\mathbb{A}^2/\mathbb{F}_p$ to $\mathbb{A}^2/\mathbb{F}_q$, its arithmetic monodromy group G_{arith} coincided with G_{geom}.

Without these "prime to p" hypotheses, we have the following result.

Theorem 3.1. *For $n \geq 2$ and $q = p^a$ a power of the odd prime p, we have the following results.*

(i) *There exists a factorization $na = AB$ and a factorization $B = bj$ such that the group G_{geom} of $\mathcal{W}(\psi, n, q)$ is $\mathrm{Sp}_{2A}(p^B) \rtimes C_b$ in one of its big Weil representations.*
(ii) *Moreover, p^j is a power of q, say $p^j = q^r$ (so that $j = ar, B = arb$), and hence we have inclusions of groups*

$$\mathrm{Sp}_{2A}(p^B) \rtimes C_b = \mathrm{Sp}_{2A}(q^{rb}) \rtimes C_b \hookrightarrow \mathrm{Sp}_{2Ab}(q^r) \hookrightarrow \mathrm{Sp}_{2Abr}(q) = \mathrm{Sp}_{2n}(q).$$

Proof. To prove (i), we argue as follows. From [KT2, Theorems 2.1, 2.2, and the argument of Proposition 4.6], we see that there exist factorizations $na = AB, B = bj$ and $na = CD, D = dk$ such that G_{geom} is a subgroup of the product group

$$(\mathrm{Sp}_{2A}(p^B) \rtimes C_b) \times (\mathrm{PSp}_{2C}(p^D) \rtimes C_d)$$

which maps onto each factor.

We apply Goursat's lemma. Note that $AB = na \geq 2$, so by Lemma 2.5(ii), the only quotient groups of $\mathrm{Sp}_{2A}(p^B) \rtimes C_b$ are

$$\mathrm{Sp}_{2A}(p^B) \rtimes C_b, \mathrm{PSp}_{2A}(p^B) \rtimes C_b, \text{ and quotients of } C_b.$$

Their commutator subgroups are

$$\mathrm{Sp}_{2A}(p^B), \mathrm{PSp}_{2A}(p^B), \{1\}$$

respectively. Similarly, the only quotient groups of $\mathrm{PSp}_{2C}(p^D) \rtimes C_d$ are

$$\mathrm{PSp}_{2C}(p^D) \rtimes C_d, \text{ and quotients of } C_d,$$

and their commutator subgroups are

$$\mathrm{PSp}_{2C}(p^D), \{1\}$$

respectively.

We first rule out the case when G_{geom} is the graph of an isomorphism between a quotient of C_b with a quotient of C_d. In this case, G_{geom} would contain the product group $\mathrm{Sp}_{2A}(p^B) \times \mathrm{PSp}_{2C}(p^D)$. This group contains elements of trace zero in the representation at hand, whereas every element of G_{arith}, and a fortiori every element of G_{geom} has nonzero trace, cf. [KT2, Proposition 4.6] and its proof.

The only remaining possibility is that G_{geom} is the graph of an isomorphism between $\mathrm{PSp}_{2A}(p^B) \rtimes C_b$ and $\mathrm{PSp}_{2C}(p^D) \rtimes C_d$. Such an isomorphism induces an isomorphism of commutator subgroups. Hence $(A, B) = (C, D)$. Comparing cardinalities, we then infer that $b = d$. Thus G_{geom} is as asserted.

To prove (ii), we use Theorem 2.4, according to which $p^j = p^{B/b}$ is the lowest value attained as the square absolute value of the trace of an element of $\mathrm{Sp}_{2A}(p^B) \rtimes C_b$ in either big Weil representation. On the other hand, from [KT2, Theorem 3.5], the group G_{arith} is also finite. The quotient G_{arith}/G_{geom} is then a finite quotient of $\mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p)$. Hence over some $\mathbb{F}_Q/\mathbb{F}_q$, we have $G_{geom} = G_{arith}$. From [KT2, Lemma 3.2], exploiting an idea of van der Geer and van der Flugt, we see that for any finite extension $k_0/\mathbb{F}_Q$, all square absolute values of traces are powers of q, and that for any point $(s, t) \in \mathbb{A}^2(k_0)$, there is a finite extension k_1/k_0 for which the same point, now viewed in $\mathbb{A}^2(k_1)$ has trace of square absolute value q^{2n}. In particular, the least square absolute value attained is some strictly positive power $q^r, r \geq 1$ of q. $\square$

We now introduce a new local system $\mathbb{W}(\psi, n, q)$ when $n \geq 3$ is **odd**, which we get by setting $t = 0$ in $\mathcal{W}(\psi, n, q)$. Thus the trace function of $\mathbb{W}(\psi, n, q)$ at a point $s \in \mathbb{A}^1(k)$, $k/\mathbb{F}_p$ a finite extension, is

$$(-1/A_k) \sum_{x \in k} \psi_k(x^{q^n+1} + sx^{q+1}).$$

On $\mathbb{A}^1/\mathbb{F}_{q^2}$, we can break up this local system as the direct sum of $q+1$ local systems, by making use of the $q+1$ multiplicative characters, including the trivial one, of order dividing $q+1$. We have

$$\mathbb{W}(\psi, n, q) = \bigoplus_{\chi \text{ with } \chi^{q+1} = \mathbb{1}} \mathcal{G}(\psi, n, q, \chi).$$

The trace function of $\mathcal{G}(\psi, n, q, \chi)$ at a point $s \in \mathbb{A}^1(k)$, $k/\mathbb{F}_{q^2}$ a finite extension, is

$$(-1/A_k) \sum_{x \in k} \psi_k(x^{\frac{q^n+1}{q+1}} + sx)\chi_k(x).$$

Here we write χ_k for $\chi \circ \mathrm{Norm}_{k/\mathbb{F}_{q^2}}$, and adopt the usual convention that for χ nontrivial, we have $\chi_k(0) = 0$, but $\mathbb{1}(0) = 1$.

These $\mathcal{G}(\psi, n, q, \chi)$ are pairwise non-isomorphic, geometrically irreducible local systems on $\mathbb{A}^1/\mathbb{F}_{q^2}$ (thanks to their descriptions as Fourier Transforms, cf. [KT1, Section

2]). The ranks of these local systems are

$$\mathrm{rank}(\mathcal{G}(\psi, n, q, \mathbb{1})) = \frac{q^n+1}{q+1} - 1,$$

$$\mathrm{rank}(\mathcal{G}(\psi, n, q, \chi)) = \frac{q^n+1}{q+1}, \chi \neq \mathbb{1}.$$

Recall that for any n, and q any power of the odd prime p, there are inclusions

$$\mathrm{SU}_n(q) \lhd \mathrm{GU}_n(q) \hookrightarrow \mathrm{Sp}_{2n}(q),$$

Theorem 3.2. *For $n \geq 3$ odd, and $q = p^a$ a power of the odd prime p, the group G_{geom} for $\mathbb{W}(\psi, n, q)$ is $\mathrm{SU}_n(q)$ in its big Weil representation (of degree q^n).*

Proof. Because $\mathbb{W}(\psi, n, q)$ is the pullback (by $(s,t) \mapsto (s,0)$) of the local system $\mathcal{W}(\psi, n, q)$, its $G_{geom,\mathbb{W}}$ is a subgroup of $G_{geom,\mathcal{W}}$. By Theorem 3.1, we have

$$G_{geom,\mathcal{W}} \hookrightarrow \mathrm{Sp}_{2n}(q).$$

Thus $G_{geom,\mathbb{W}}$ is a subgroup of $\mathrm{Sp}_{2n}(q)$ under which a big Weil representation of $\mathrm{Sp}_{2n}(q)$ breaks up into $q+1$ pieces, one of rank $\frac{q^n-q}{q+1}$ and q of rank $\frac{q^n+1}{q+1}$. By Theorem 2.3, we have inclusions

$$\mathrm{SU}_n(q) \leq G_{geom,\mathbb{W}} \leq \mathrm{GU}_n(q).$$

The group $\mathrm{GU}_n(q)$ has a quotient, via the determinant, of order $q+1$, which is prime to p. Because $G_{geom,\mathbb{W}}$ is the monodromy group of a local system on $\mathbb{A}^1/\overline{\mathbb{F}_p}$, it has no nontrivial prime to p quotients. Thus we have $G_{geom,\mathbb{W}} = \mathrm{SU}_n(q)$. ☐

Theorem 3.3. *For $n \geq 3$ odd and q an odd prime power, the geometric monodromy group $G_{geom,\mathcal{W}}$ of $\mathcal{W}(\psi, n, q)$ is $\mathrm{Sp}_{2n}(q)$ in one of its big Weil representations $\mathsf{Weil}_{1,2}$ (of degree q^n). Moreover, after extension of scalars to $\mathbb{A}^2/\mathbb{F}_q$, we have $G_{geom} = G_{arith}$.*

Proof. Recall the inclusion

$$\mathrm{SU}_n(q) = G_{geom,\mathbb{W}} \leq G_{geom,\mathcal{W}} = \mathrm{Sp}_{2A}(p^B) \rtimes C_b$$

and the relation $n = Abr$ of Theorem 3.1. By Lemma 2.5(i), $br \leq 2$, but $2 \nmid n$, hence $ar = 1$ and $(A, p^B, b) = (n, q, 1)$, yielding the first assertion.

Once $G_{geom,\mathcal{W}} = \mathrm{Sp}_{2n}(q) = \mathrm{Sp}_{2n}(p^a)$, $G_{arith,\mathcal{W}}$ is contained in $\mathrm{Sp}_{2n}(p^a) \rtimes C_a$, cf. [KT2, proof of Lemma 4.7]. Thus the quotient $G_{arith,\mathcal{W}}/G_{geom,\mathcal{W}}$ has order dividing a, so after extension of scalars to $\mathbb{A}^2/\mathbb{F}_p$ to $\mathbb{A}^2/\mathbb{F}_{p^a} = \mathbb{A}^2/\mathbb{F}_q$ we have $G_{geom} = G_{arith}$. ☐

Theorem 3.4. *For $n \geq 3$ odd and q a power of the odd prime p, the geometric monodromy group of the local system $\mathcal{G}(\psi, n, q, \mathbb{1})$ is $\mathrm{PSU}_n(q)$, the image of $\mathrm{SU}_n(q)$ in its unique irreducible representation of dimension $\frac{q^n-q}{q+1}$, with character $\zeta_{0,n}$. The geometric monodromy group of $\mathcal{G}(\psi, n, q, \chi_2)$ (where χ_2 is the quadratic character) is the image of $\mathrm{SU}_n(q)$ in its unique orthogonal representation of dimension $\frac{q^n+1}{q+1}$, with character $\zeta_{(q+1)/2,n}$. For the remaining $q-1$ local systems $\mathcal{G}(\psi, n, q, \chi)$ with χ^2*

nontrivial, $\chi^{q+1} = \mathbb{1}$*, their geometric monodromy groups are the images of* $\mathrm{SU}_n(q)$ *in its* $q-1$ *non-selfdual irreducible representations of dimension* $\frac{q^n+1}{q+1}$*.*

Proof. Because $G_{geom,\mathbb{W}}$ is $\mathrm{SU}_n(q)$, the geometric monodromy groups in question are quotients of $\mathrm{SU}_n(q)$ in various of its irreducible representations. Recall the fact [TZ1, Theorem 4.1] that $\mathrm{SU}_n(q)$ has, up to equivalence, one irreducible representation of dimension $\frac{q^n-q}{q+1}$ (with character $\zeta_{0,n}$) and q irreducible representations of dimension $\frac{q^n+1}{q+1}$ (with character $\zeta_{j,n}$, $1 \le j \le q$), with exactly one of the q latter representations being self-dual (and necessarily orthogonal, as it has odd dimension). Using this fact and looking at the dimensions, we get the asserted matching. □

Corollary 3.5. *After extension of scalars to* $\mathbb{A}^1/\mathbb{F}_{q^{2(q+1)}}$*, we have*

$$G_{geom,\mathbb{W}} = G_{arith,\mathbb{W}}$$

for $\mathbb{W}(\psi, n, q)$*. The same is true for each of the* $q+1$ *local systems* $\mathcal{G}(\psi, n, q, \chi)$*.*

Proof. After extension of scalars to $\mathbb{A}^1/\mathbb{F}_q$, we have $G_{arith,\mathcal{W}} = \mathrm{Sp}_{2n}(q)$, and hence

$$G_{arith,\mathbb{W}} \le \mathrm{Sp}_{2n}(q).$$

By Theorem 2.3, which we may apply after further extension of scalars to $\mathbb{A}^1/\mathbb{F}_{q^2}$, we have

$$\mathrm{SU}_n(q) \le G_{arith,\mathbb{W}} \le \mathrm{GU}_n(q).$$

As we have $G_{geom,\mathbb{W}} = \mathrm{SU}_n(q)$, we see that the quotient $G_{arith,\mathbb{W}}/G_{geom,\mathbb{W}}$ has order dividing $q+1$. Thus after extension of scalars to $\mathbb{A}^1/\mathbb{F}_{q^{2(q+1)}}$, we have $G_{geom,\mathbb{W}} = G_{arith,\mathbb{W}}$. Each of the irreducible constituents then has $G_{geom} = G_{arith}$ as well. □

Remark 3.6. Theorem 3.3 is an improvement, in the n odd case, of Theorem 1.1 of [KT2, Theorem 1.1, 4.8], which required that both n and $a := \log_p(q)$ be prime to p. Theorem 3.4 verifies the G_{geom} conjectures of [KT1, Conjecture 9.2] in the case that q is odd. Corollary 3.5 establishes a weak version of the G_{arith} conjectures of [KT1, Conjecture 9.2], again in the case when q is odd. We should also point out that the normalizing factor A_k used here to define the local systems $\mathcal{G}(\psi, n, q, \chi)$ here can differ by a sign from the normalizing factors β used to define these local systems in [KT1, Lemma 8.3]. Over $\mathbb{F}_{q^2}$, each normalizing factor is either q or $-q$, so over extensions of $\mathbb{F}_{q^4}$ there is no conflict. But we cannot hope to have the conjectural equality of G_{geom} with G_{arith} over $\mathbb{F}_{q^2}$ for both $\mathcal{G}(\psi, n, q, \chi)$ as normalized here and for $\mathcal{G}(\psi, n, q, \chi)$ as normalized in [KT1, Lemma 8.3] in any situation where the normalizing factors do in fact differ by a sign.

The virtue of the normalizing factors β is that with them, when we work over $\mathbb{F}_{q^2}$, the group G_{arith} for the renormalized $\mathcal{G}(\psi, n, q, \chi)$ lands in $\mathrm{Sp}(\frac{q^n-q}{q+1}, \overline{\mathbb{Q}}_\ell)$ for $\chi = \mathbb{1}$, it lands in $\mathrm{SO}(\frac{q^n+1}{q+1}, \overline{\mathbb{Q}}_\ell)$ for $\chi = \chi_2$ the quadratic character, and it lands in $\mathrm{SL}(\frac{q^n+1}{q+1}, \overline{\mathbb{Q}}_\ell)$ for the χ with $\chi^2 \neq \mathbb{1}$. So with the exception of the $\chi = \mathbb{1}$ case, where a sign change of normalizing factor won't alter landing in $\mathrm{Sp}(\frac{q^n-q}{q+1}, \overline{\mathbb{Q}}_\ell)$, any sign change of normalizing factor in the other cases will destroy landing in SL (simply because $\frac{q^n+1}{q+1}$ is odd).

In the case of the quadratic character χ_2, there is no sign change: the β over $\mathbb{F}_{q^2}$ is equal to $A_{\mathbb{F}_{q^2}}$. Indeed, that β is, cf. [KT1, Lemma 8.3 (3)],

$$\beta := -(-1)^{(q+1)/2}q = (-1)^{(q-1)/2}q = (A^2_{\mathbb{F}_p})^{\deg(\mathbb{F}_q/\mathbb{F}_p)} = A_{\mathbb{F}_{q^2}}.$$

[The normalizing factor β for the renormalized $\mathcal{G}(\psi, n, q, \chi)$ is $-(-1)^{(q+1)/m}q$ for m the order of χ. This will be equal to $A_{\mathbb{F}_{q^2}}$ precisely when $(q+1)/2$ and $(q+1)/m$ have the same parity.]

For $\mathcal{G}(\psi, n, q, \mathbb{1})$, we have

$$G_{geom} = \Psi_0(\mathrm{SU}_n(q)), \quad G_{geom} \le G_{arith} \le \Psi_0(\mathrm{GU}_n(q)).$$

So we see from Lemma 2.1(i) that it suffices to extend scalars from $\mathbb{F}_{q^2}$ to $\mathbb{F}_{q^{2\cdot\gcd(n,q+1)}}$ (instead of to $\mathbb{F}_{q^{2(q+1)}}$) to achieve $G_{geom} = G_{arith}$ for $\mathcal{G}(\psi, n, q, \mathbb{1})$.

For $\mathcal{G}(\psi, n, q, \chi_2)$, we have

$$G_{geom} = \Psi_{(q+1)/2}(\mathrm{SU}_n(q)), \quad G_{geom} \le G_{arith} \le \Psi_{(q+1)/2}(\mathrm{GU}_n(q)) \cap \mathrm{SO}_{(q^n+1)/(q+1)}(\overline{\mathbb{Q}_\ell}).$$

So we see from Lemma 2.1(iii) that for $\mathcal{G}(\psi, n, q, \chi_2)$, it suffices to extend scalars from $\mathbb{F}_{q^2}$ to $\mathbb{F}_{q^{q+1}}$ (instead of to $\mathbb{F}_{q^{2(q+1)}}$) to achieve $G_{geom} = G_{arith}$. Both these statements are far from the conjectured equality $G_{geom} = G_{arith}$ over $\mathbb{F}_{q^2}$ (except, of course, in the special case when $\gcd(n, q+1) = 1$).

4. Moments of Weil representations of odd-dimensional unitary groups

In this section, we will consider special unitary groups $G := \mathrm{SU}_n(q) = \mathrm{SU}(W)$ where q is any prime power. The main result is Theorem 4.11 showing that when $n \ge 3$ is odd, the Weil representations of G have n^{th} moment 1 or 0.

First we assume that $n = 2k+1 \ge 5$ is odd, and fix a basis $(e_1, \dots, e_k, f_1, \dots, f_k, w)$ of the Hermitian space $W = \mathbb{F}^n_{q^2}$, in which the Hermitian form $\circ$ takes values

$$e_i \circ e_j = f_i \circ f_j = e_i \circ w = f_i \circ w = 0,\ e_i \circ f_j = \delta_{i,j},\ w \circ w = 1. \tag{4.0.1}$$

We also fix the notation

$$P_1 := \mathrm{Stab}_G(\langle e_1 \rangle_{\mathbb{F}_{q^2}}) = Q_1 L_1,\ P_k := \mathrm{Stab}_G(\langle e_1, \dots, e_k \rangle_{\mathbb{F}_{q^2}}) = Q_k L_k,$$

where $Q_1 = \mathbf{O}_p(P_1)$, $Q_k = \mathbf{O}_p(P_k)$, $L_k \cong \mathrm{GL}_k(q^2)$. The action of any $X \in L_k = \mathrm{GL}_k(q^2)$ in the indicated basis of W is given by $\mathrm{diag}(X, {}^tX^{-q}, \det(X)^{q-1})$, see [ST, §5.1].

As shown in [GMST, Lemmas 12.5, 12.6], the Levi subgroup L has a unique orbit $\mathcal{O}$ on $\mathrm{Irr}(\mathbf{Z}(Q_k)) \smallsetminus \{1_{\mathbf{Z}(Q_k)}\}$ of smallest length $(q^{2k}-1)/(q+1)$, which then occurs in the restriction of any Weil character $\zeta_{i,n}$. Moreover, any $\lambda \in \mathcal{O}$ can only lie under an irreducible character of degree q of Q_k. In particular, this shows that

Lemma 4.1. *Suppose $n = 2k+1 \geq 5$. Then $\zeta_{0,n}$ is irreducible over P_k. If $1 \leq i \leq q$, then $\zeta_{i,n}|_{P_k} = \nu_i + \theta_i$, where $\theta_i \in \mathrm{Irr}(P_k)$ affords the orbit $\mathcal{O}$, and ν_i is a linear character of P_k trivial at $\mathbf{Z}(Q_k)$.*

Lemma 4.2. *In the notation of Lemma 4.1, assume that $1 \leq i \leq q$. Then $\mathrm{Ker}(\nu_i) \geq Q_k$, and if $X \in L_k$ has determinant σ^t as an element in $\mathrm{GL}_k(q^2)$ with $t \in \mathbb{Z}$, then $\nu_i(X) = \boldsymbol{\sigma}^{(q-1)it}$.*

Proof. As noted in Lemma 4.1, ν_i is trivial at $\mathbf{Z}(Q_k)$, and it is P_k-invariant. But L_k acts transitively on the $q^{2k}-1$ nontrivial linear characters of $Q_k/\mathbf{Z}(Q_k)$, so $\mathrm{Ker}(\nu_i) \geq Q_k$. Next, $[L_k, L_k] \cong \mathrm{SL}_k(q^2)$ is perfect, so ν_i is trivial at $[L_k, L_k]$. Thus there is some $0 \leq s \leq q^2 - 2$ such that $\nu_i(X) = \boldsymbol{\sigma}^{ts}$ for the listed $X \in L_k$. To find s, it suffices to evaluate $\nu_i(X)$ for some X_0 that generates L_k modulo $[L_k, L_k]$. Let γ be a generator of $\mathbb{F}_{q^{2k}}^\times$ such that $\gamma^{(q^{2k}-1)/(q^2-1)} = \sigma$, and choose $X_0 \in L_k$ conjugate to

$$\mathrm{diag}(\gamma, \gamma^{q^2}, \ldots, \gamma^{q^{2k-2}})$$

over $\overline{\mathbb{F}}_q$, so that $\det(X_0) = \sigma$. Since no eigenvalue of X_0 belongs to $\mathbb{F}_{q^2}$, X_0 cannot fix any $\lambda \in \mathcal{O}$, see formula (20) of [ST]), and so $\theta_i(X_0) = 0$ and $\nu_i(X_0) = \zeta_{i,n}(X_0)$. The absence of eigenvalues in $\mathbb{F}_{q^2}$ and the equality $\det(X_0)^{q-1} = \rho$ imply by (2.0.2) that $\zeta_{i,n}(X_0) = \boldsymbol{\rho}^i = \boldsymbol{\sigma}^{(q-1)i}$, i.e. $s = (q-1)i$ as stated. $\square$

Proposition 4.3. *Suppose $n = 2k+1 \geq 5$. Then $(\zeta_n)^{n-1}$ contains $\zeta_{i,n}$ with multiplicity one if $i > 0$, and zero if $i = 0$.*

Proof. Note that $(\zeta_n)^2$ is just the permutation character of G acting on the point set of W. Hence $(\zeta_n)^{n-1}$ is the permutation character of G acting on the set Ω of ordered k-tuples $\omega = (v_1, \ldots, v_k)$, $v_i \in W$. Let $\pi_\omega = \mathrm{Ind}_{G_\omega}^G(1_{G_w})$ denote the permutation character of G acting on the G-orbit of $\omega = (v_1, \ldots, v_k)$, where $G_\omega = \mathrm{Stab}_G(\omega)$, and suppose that $\zeta_{i,n}$ is an irreducible constituent of π_ω. Then

$$0 < [\pi_\omega, \zeta_{i,n}]_G = [1_{G_\omega}, \zeta_{i,n}|_{G_\omega}]_{G_\omega}; \tag{4.3.1}$$

in particular, 1_{G_ω} is an irreducible constituent of $\zeta_{i,n}|_{G_\omega}$.

(i) First we consider the case where $X := \langle v_1, \ldots, v_k \rangle_{\mathbb{F}_{q^2}}$ is contained in a non-degenerate subspace Y of W of codimension ≥ 2. Without loss we may assume that $e_1, f_1 \in Y^\perp$. Then G_ω contains a natural subgroup $M := \mathrm{SU}(\langle e_1, f_1 \rangle_{\mathbb{F}_{q^2}}) \cong \mathrm{SU}_2(q)$ (that acts trivially on Y). The branching rule (2.0.3) then shows that $\zeta_{i,n}|_M$ is a sum of Weil characters $\zeta_{j,2}$ of M. As mentioned above, an irreducible constituent λ of $\zeta_{j,2}$ can have degree 1 only when $(q, j) = (2, \neq 0)$ or $(q, j) = (3, (q+1)/2)$. In the former case, one can check that λ is actually the sign character of $M = \mathrm{SU}_2(2) \cong \mathrm{Sym}_3$. In the latter case, $\lambda(z) \neq 1$ for some element z of $M \cong \mathrm{SU}_2(3)$ of order 3. Thus λ can never be equal to 1_M, contradicting (4.3.1).

In particular, we have shown that X cannot be non-degenerate.

(ii) Suppose now that $0 \neq X \cap X^\perp$ has dimension $j \leq k-1$. By Witt's lemma, we may then assume that $X = \langle e_1, \ldots, e_j, w_1, \ldots, w_{k-j} \rangle_{\mathbb{F}_{q^2}}$, where $\langle w_1, \ldots, w_{k-j} \rangle_{\mathbb{F}_{q^2}}$ is a non-degenerate subspace of

$$\langle e_{j+1}, \ldots, e_k, f_{j+1}, \ldots, f_k \rangle_{\mathbb{F}_{q^2}}.$$

But then X is contained in the non-degenerate subspace

$$Y := \langle e_1, \ldots, e_j, f_1, \ldots, f_j, w_1, \ldots, w_{k-j} \rangle_{\mathbb{F}_{q^2}}$$

of codimension $n - (k+j) \geq 2$, contradicting (i).

(iii) We have shown that $\dim(X \cap X^\perp) = k$, i.e. X is totally singular of dimension k. There is only one G-orbit of such ω, and we may assume that $\omega = (e_1, \ldots, e_k)$. The description of P_k given in [ST, §5.1] shows that $G_\omega = Q_k$. Now Lemmas 4.1, 4.2, and (4.3.1) show that $[\pi_\omega, \zeta_{i,n}]_G = 1 - \delta_{0,i}$, as stated. □

Next we define the following linear characters λ_i of the parabolic subgroup $P_1 = \mathrm{Stab}_G(\langle e_1 \rangle_{\mathbb{F}_{q^2}})$ for $1 \leq i \leq q$: if $g \in P_1$ sends e_1 to σ^t for $0 \leq t \leq q^2 - 2$, then $\lambda_i(g) = \boldsymbol{\sigma}^{-(q-1)it}$, and set

$$\Lambda_i := \mathrm{Ind}_{P_1}^G(\lambda_i).$$

Proposition 4.4. *Suppose $n = 2k+1 \geq 5$, $(n,q) \neq (5,2)$, and $1 \leq i \leq q$. Then Λ_i enters the character $(\zeta_n)^2$, and $[(\zeta_{i,n})^2, \Lambda_i] \geq 1$.*

Proof. (i) As discussed in [GMST, §11], $P_1' := \mathrm{Stab}_G(e_1) = Q_1 \rtimes L_1'$, where $L_1' = \mathrm{Stab}_G(e_1) \cap \mathrm{Stab}_G(f_1) \cong \mathrm{SU}_{n-2}(q)$. Note that Λ_i enters the character $\mathrm{Ind}_{P_1'}^{P_1}(1_{P_1'})$, which in turn enters the character $(\zeta_n)^2$. Furthermore, L_1 acts transitively on the $q-1$ nontrivial linear characters of $\mathbf{Z}(Q_1)$ (which has order q), and for each such character α there is a unique irreducible character of Q_1 of degree q^{n-2}, which then extends to a unique character M_α of P_1'. We fix some nontrivial $\alpha \in \mathrm{Irr}(\mathbf{Z}(Q_1))$ and let $K := \mathrm{Stab}_{P_1}(\alpha) = P_1' \cdot C_{q+1}$. By its uniqueness, M_α extends to K. Note that

$$\zeta_{i,n}(1) = (q^n+1)/(q+1) < 2q^{n-2}(q-1) = 2(q-1)M_\alpha(1).$$

It follows by Clifford's theorem that

$$\zeta_{i,n}|_{P_1} = \beta_i + \mathrm{Ind}_K^{P_1}(M_\alpha), \tag{4.4.1}$$

for some extension to K of M_α which we also denote by M_α, and for some character β_i of P_1 of degree $(q^{n-2}+1)/(q+1)$, with $\mathbf{Z}(Q_1) \leq \mathrm{Ker}(\beta_i)$. Next, $M_\alpha|_{L_1'} = \zeta_{n-2}$. Applying (2.0.3) to the standard subgroup L_1' and using (4.4.1), we get

$$\beta_i|_{L_1'} = \zeta_{i,n}|_{L_1'} - (q-1)\zeta_{n-2} = \sum_{j \neq i,\ j' \neq j} \zeta_{n-2,j'} - (q-1)\sum_{j'=0}^{q} \zeta_{n-2,j'} = \zeta_{n-2,i}.$$

In particular, $\beta_i \in \mathrm{Irr}(P_1)$.

(ii) As usual, $\bar{\chi}$ denotes the complex conjugate of any character χ. Note that $\mathrm{Stab}_{P_1}(\bar{\alpha}) = K$. Hence, (4.4.1) implies that

$$\overline{\zeta}_{i,n}|_{P_1} = \overline{\beta}_i + \mathrm{Ind}_K^{P_1}(\overline{M}_\alpha). \tag{4.4.2}$$

Observe that $\overline{M}_\alpha$ affords the $\mathbf{Z}(Q_1)$-character $q^{n-2}\bar{\alpha}$ and is irreducible over P_1'. By the aforementioned uniqueness, $\overline{M}_\alpha$ agrees with $M_{\bar{\alpha}}$ on P_1', where $M_{\bar{\alpha}}$ is the K-character of the $\bar{\alpha}$-isotypic component in $\zeta_{i,n}|_{P_1}$. As $K/P_1 \cong C_{q+1}$, these two characters differ from each other by a linear character of K/P_1', which extends to a linear character δ of $P_1/P_1' \cong C_{q^2-1}$. We have shown that

$$\mathrm{Ind}_K^{P_1}(\overline{M}_\alpha) = \mathrm{Ind}_K^{P_1}(M_{\bar{\alpha}} \cdot \delta|_K) = \mathrm{Ind}_K^{P_1}(M_{\bar{\alpha}}) \cdot \delta. \tag{4.4.3}$$

and

$$\zeta_{i,n}|_{P_1} = \beta_i + \mathrm{Ind}_K^{P_1}(M_{\bar{\alpha}}), \tag{4.4.4}$$

(iii) We aim to show that we one can take $\delta = \overline{\lambda}_i$ in (4.4.3). Let τ be an element of $\mathbb{F}_{q^{4k-2}}^\times$ of order $q^{2k-1}+1$ chosen such that $\tau^{(q^{2k-1}+1)/(q+1)} = \rho$. Then we can find an element $h \in K$ such that $h(e_1) = \rho e_1$ and h is conjugate to

$$\mathrm{diag}(\rho, \rho, \tau^{-2}, \tau^{2q}, \tau^{-2q^2}, \ldots, \tau^{-2(-q)^{2k-2}})$$

over $\overline{\mathbb{F}}_{q^2}$. Since $k \geq 2$ and $(k,q) \neq (2,2)$, by [Zs] there is a prime divisor ℓ of $q^{4k-2}-1$ that does not divide $\prod_{j=1}^{4k-3}(q^j-1)$. In particular, ℓ divides $(q^{2k-1}+1)$, and moreover the ℓ-part of $|P_1|$ is equal to the ℓ-part of $\beta_i(1)$, whence β_i is an irreducible character of P_1 of ℓ-defect zero. On the other hand, for any $1 \leq t \leq q$, ℓ divides $|h^t|$, whence $\beta_i(t) = 0$, and so we obtain by using (2.0.2), (4.4.2), (4.4.4) that

$$\mathrm{Ind}_K^{P_1}(M_{\bar{\alpha}})(h^t) = \zeta_{i,n}(h^t) = -(q-1)\boldsymbol{\rho}^{it},$$
$$\mathrm{Ind}_K^{P_1}(\overline{M}_\alpha)(h^t) = \overline{\zeta}_{i,n}(h^t) = -(q-1)\boldsymbol{\rho}^{-it}.$$

It now follows from (4.4.3) that

$$\delta(h^t) = \boldsymbol{\rho}^{-2it} = \boldsymbol{\rho}^{(q-1)it} = \overline{\lambda}_i(h^t),$$

whence $\delta(g) = \overline{\lambda}_i(g)$ for all $g \in K$, since the choice of h ensures that h generates K modulo P_1'. Together with (4.4.3), we have shown that

$$(\mathrm{Ind}_K^{P_1}(M_{\bar{\alpha}}) \cdot \delta)(g) = (\mathrm{Ind}_K^{P_1}(M_{\bar{\alpha}}) \cdot \overline{\lambda}_i)(g) \tag{4.4.5}$$

for all $g \in K$. If $g \in P_1 \smallsetminus K$ then $\mathrm{Ind}_K^{P_1}(M_{\bar{\alpha}})(g) = 0$ since $K \lhd P_1$, and so (4.4.5) holds for g as well. Consequently,

$$\mathrm{Ind}_K^{P_1}(\overline{M}_\alpha) = \mathrm{Ind}_K^{P_1}(M_{\bar{\alpha}}) \cdot \overline{\lambda}_i.$$

This identity, together with (4.4.2) and (4.4.4), implies by Frobenius' reciprocity that

$$\begin{aligned}[(\zeta_{i,n})^2, \Lambda_i]_G &= [\zeta_{i,n}\overline{\Lambda}_i, \overline{\zeta}_{i,n}]_G = [\zeta_{i,n} \cdot \mathrm{Ind}_{P_1}^G(\overline{\lambda}_i), \overline{\zeta}_{i,n}]_G \\ &= [\mathrm{Ind}_{P_1}^G(\zeta_{i,n}|_{P_1} \cdot \overline{\lambda}_i), \overline{\zeta}_{i,n}]_G = [\zeta_{i,n}|_{P_1} \cdot \overline{\lambda}_i, \overline{\zeta}_{i,n}]_{P_1} \\ &\geq [\mathrm{Ind}_K^{P_1}(M_{\tilde{\alpha}}) \cdot \overline{\lambda}_i, \mathrm{Ind}_K^{P_1}(\overline{M}_\alpha)]_{P_1} = 1,\end{aligned}$$

as stated. □

Proposition 4.5. *Suppose $n = 2k+1 \geq 5$ and $0 < i \leq q$. Then $[(\Lambda_i)^k, \overline{\zeta}_{i,n}] = 1$.*

Proof. Recall G acts transitively on the set Ξ of isotropic 1-spaces in $W = \mathbb{F}_{q^2}^n$, with $P_1 = \mathrm{Stab}_G(\pi_1)$, where we set $\pi_j := \langle e_j \rangle_{\mathbb{F}_{q^2}}$ for $1 \leq j \leq k$. Hence the character Λ_i is afforded by a $\mathbb{C}G$-module

$$V = \mathrm{Ind}_{P_1}^G(V_{\pi_1}) = \oplus_{gP_1 \in G/P_1} V_{g(\pi_1)},$$

where $V_{\pi_1} = \langle v_{\pi_1} \rangle_{\mathbb{C}}$ is a one-dimensional P_1-module with character λ_i, and G permutes the summands via $h(V_{g(\pi_1)}) = V_{hg(\pi_1)}$. It follows that $(\Lambda_i)^k$ is afforded by the G-module

$$V^{\otimes k} = \langle v_\xi \mid \xi \in \Xi^k \rangle_{\mathbb{C}},$$

where $v_\xi = v_{\xi_1} \otimes v_{\xi_2} \otimes \ldots \otimes v_{\xi_k}$ for $\xi = (\xi_1, \xi_2, \ldots, \xi_k)$.

Consider the G-orbit Π of the k-tuple $\pi := (\pi_1, \pi_2, \ldots, \pi_k) \in \Xi^k$. Then the G-submodule

$$V(\Pi) := \langle v_\xi \mid \xi \in \Pi \rangle_{\mathbb{C}}$$

of $V^{\otimes k}$ affords the character $\mathrm{Ind}_R^G(\mu)$, where $R := \cap_{j=1}^k \mathrm{Stab}_G(\langle e_j \rangle_{\mathbb{F}_{q^2}})$, and

$$\mu(h) = \boldsymbol{\sigma}^{-(q-1)i\sum_{j=1}^k t_j}$$

if $h(e_j) = \sigma^{t_j}$ for $0 \leq t_j \leq q^2 - 2$ and $1 \leq j \leq k$.

Note that $Q_k \lhd R < P_k$ and $Q_k \leq \mathrm{Ker}(\mu)$. Furthermore, if $h \in L_k$ belongs to R and $h(e_j) = \sigma^{t_j}$, then $\det(h)$ (as an element in $\mathrm{GL}_k(q^2)$ is $\sigma^{\sum_{j=1}^k t_j}$, and so

$$\overline{\nu}_i(h) = \boldsymbol{\sigma}^{-(q-1)i\sum_{j=1}^k t_j} = \mu(h)$$

for the character ν_i considered in Lemma 4.2, i.e. $\overline{\nu}_i|_R = \mu$. By Lemma 4.1, we have therefore shown that

$$0 < [\mu, \overline{\zeta}_{i,n}|_R]_R = [\mathrm{Ind}_R^G(\mu), \overline{\zeta}_{i,n}]_G \leq [(\Lambda_i)^k, \overline{\zeta}_{i,n}]_G.$$

On the other hand, $(\Lambda_i)^k$ enters the character $(\zeta_n)^{n-1}$ by Proposition 4.4, whence the upper bound $[(\Lambda_i)^k, \overline{\zeta}_{i,n}] \leq 1$ follows from Proposition 4.3. □

Next we will study some *see-saw dual pairs* (cf. [Ku]) to determine various branching rules. Our consideration is based on the following well-known formula [LBST, Lemma 5.5]:

Lemma 4.6. *Let ω be a character of the direct product $S \times G$ of finite groups S and G. Then*

$$\omega = \sum_{\alpha \in \mathrm{Irr}(S)} D_\alpha \otimes \alpha,$$

where

$$D_\alpha : g \mapsto \frac{1}{|S|} \sum_{x \in S} \overline{\alpha(x)} \omega(xg)$$

is either zero, or a character of G.

We will work with a finite group Γ that contains two dual pairs $S_1 \times G_1$ and $S_2 \times G_2$, where $G_1 \geq G_2$ and $S_2 \geq S_1$.

Lemma 4.7. *Let ω be a character of Γ, and decompose*

$$\omega|_{G_1 \times S_1} = \sum_{\alpha \in \mathrm{Irr}(S_1)} D_\alpha \otimes \alpha, \ \omega|_{G_2 \times S_2} = \sum_{\gamma \in \mathrm{Irr}(G_2)} \gamma \otimes E_\gamma$$

as in Lemma 4.6. Then, for any $\alpha \in \mathrm{Irr}(S_1)$ and any $\gamma \in \mathrm{Irr}(G_2)$ we have that

$$[D_\alpha|_{G_2}, \gamma]_{G_2} = [\alpha, E_\gamma|_{S_1}]_{S_1},$$

and hence

$$D_\alpha|_{G_2} = \sum_{\gamma \in \mathrm{Irr}(G_2)} [E_\gamma|_{S_1}, \alpha]_{S_1} \cdot \gamma.$$

Proof. Write $a_{\alpha,\gamma} := [D_\alpha|_{G_2}, \gamma]_{G_2}$, so that

$$D_\alpha|_{G_2} = \sum_{\gamma \in \mathrm{Irr}(G_2)} a_{\alpha,\gamma} \gamma.$$

Then

$$\begin{aligned} \omega|_{G_2 \times S_1} &= \sum_{\alpha \in \mathrm{Irr}(S_1),\ \gamma \in \mathrm{Irr}(G_2)} a_{\alpha,\gamma} \gamma \otimes \alpha \\ &= \sum_{\gamma \in \mathrm{Irr}(G_2)} \gamma \otimes \sum_{\alpha \in \mathrm{Irr}(S_1)} a_{\alpha,\gamma} \alpha. \end{aligned}$$

Thus $E_\gamma|_{S_1} = \sum_{\alpha \in \mathrm{Irr}(S_1)} a_{\alpha,\gamma} \alpha$, and the statements follow. □

First we consider the dual pair

(4.7.1) $$G_2 \times S_2$$

inside $\Gamma := \mathrm{GU}_{2n}(q)$, where $S_2 = \mathrm{GU}_2(q)$ and $G_2 = \mathrm{SU}_n(q)$, and $\omega = \zeta_{2n} = \zeta_{2n,q}$. More precisely, we view S_2 as $\mathrm{GU}(U)$, where $U = \langle v_1, v_2 \rangle_{\mathbb{F}_{q^2}}$ is endowed with the Hermitian form $\circ$, with an orthonormal basis (v_1, v_2). Next, $G_2 = \mathrm{SU}_n(q)$ is $\mathrm{SU}(W)$, where $W = \mathbb{F}_{q^2}^n$ is endowed with the Hermitian form $\circ$ defined in (4.0.1). Now we consider $V = U \otimes_{\mathbb{F}_{q^2}} W$ with the Hermitian form $\circ$ defined via

$$(u \otimes w) \circ (u' \otimes w') = (u \circ u')(w \circ w')$$

for $u \in U$ and $w \in W$. The action of $G_2 \times S_2$ on V induces a homomorphism $G_2 \times S_2 \to \Gamma := \mathrm{GU}(V)$.

Now V is the orthogonal sum $V_1 \oplus V_2$, where $V_i := v_i \otimes W$. This gives us a subgroup

$$G_1 := \mathrm{SU}(V_1) \times \mathrm{SU}(V_2) \cong \mathrm{SU}_n(q) \times \mathrm{SU}_n(q)$$

of Γ that contains (the image of) G_2. In fact, G_2 embeds diagonally in G_1: $g \mapsto \mathrm{diag}(g, g)$. Next,

$$S_1 := \mathrm{GU}(\langle v_1 \rangle_{\mathbb{F}_{q^2}}) \times \mathrm{GU}(\langle v_2 \rangle_{\mathbb{F}_{q^2}}) \cong \mathrm{GU}_1(q) \times \mathrm{GU}_1(q)$$

is just the non-split diagonal torus of S_2.

In the above basis (v_1, v_2) of U and for $0 \le i, j \le q$, we consider the character

$$\lambda_{i,j} : \mathrm{diag}(\rho^a, \rho^b) \mapsto \boldsymbol{\rho}^{ia+jb}$$

of S_1. Then, as explained in [TZ2, §4], $\zeta_{i,n}$ corresponds to the $\boldsymbol{\rho}^i$-eigenspace of the generator $\rho \cdot 1_W$ of $\mathbf{Z}(\mathrm{GU}_n(q))$, so that

$$D_{\lambda_{ij}} = \zeta_{i,n} \otimes \zeta_{j,n} \tag{4.7.2}$$

for the dual pair $G_1 \times S_1$.

We use the notation of [E] for the irreducible characters of $S_2 = \mathrm{GU}_2(q)$ (with the parameter $q+1$ in the superscripts of characters changed to 0). For instance

$$\chi_1^{(t)}|_{S_1} = \lambda_{t,t}.$$

The decomposition

$$\omega|_{S_2 \times G_2} = \sum_{\alpha \in \mathrm{Irr}(S_2)} \alpha \otimes C_\alpha \tag{4.7.3}$$

was described in [LBST, Proposition 6.3]. In particular, the G_2-characters

$$C_\alpha^\circ := C_\alpha - k_\alpha \cdot 1_{G_2}, \tag{4.7.4}$$

where $\alpha \in \mathrm{Irr}(S_2)$, are irreducible and pairwise distinct, and $k_\alpha \in \{0, 1\}$ is listed in Table I.

This implies

Corollary 4.8. *For the decomposition*

$$\omega|_{G_2 \times S_2} = \sum_{\gamma \in \mathrm{Irr}(G_2)} \gamma \otimes E_\gamma,$$

TABLE I. Degrees of C°_α for $G_2 = \mathrm{SU}_n(q)$

α	$\alpha(1)$	$C^\circ_\alpha(1)$	k_α
$\chi_1^{(0)}$	1	$(q^n-(-1)^n)(q^{n-1}+(-1)^n q^2)/(q+1)(q^2-1)$	1
$\chi_1^{(t)}$, $t \neq 0$	1	$(q^n-(-1)^n)(q^{n-1}+(-1)^n)/(q+1)(q^2-1)$	0
$\chi_q^{(0)}$	q	$(q^n+(-1)^n q)(q^n-(-1)^n q^2)/(q+1)(q^2-1)$	1
$\chi_q^{(t)}$, $t \neq 0$	q	$(q^n-(-1)^n)(q^n+(-1)^n q)/(q+1)(q^2-1)$	0
$\chi_{q-1}^{(0,u)}$, $u \neq 0$	$q-1$	$(q^n-(-1)^n)(q^{n-1}-(-1)^n q)/(q+1)^2$	0
$\chi_{q-1}^{(t,u)}$, $t,u \neq 0$	$q-1$	$(q^n-(-1)^n)(q^{n-1}+(-1)^n)/(q+1)^2$	0
$\chi_{q+1}^{(t)}$	$q+1$	$(q^n-(-1)^n)(q^{n-1}+(-1)^n)/(q^2-1)$	0

we have that

$$E_\gamma = \begin{cases} \alpha, & \gamma = C^\circ_\alpha \text{ for some } \alpha \in \mathrm{Irr}(S_2), \\ \chi_1^{(0)} + \chi_q^{(0)}, & \gamma = 1_{G_2}, \\ 0, & \text{otherwise.} \end{cases}$$

Proposition 4.9. *Suppose $n = 2k+1 \geq 5$ and $(n,q) \neq (5,2)$. For $0 < i \leq q$, and in the notation of* (4.7.3)–(4.7.4) *we have*

$$\Lambda_i = C_{\chi_1^{(i)}} + C_{\chi_q^{(i)}}.$$

Among these two irreducible constituents, only $C_{\chi_1^{(i)}}$ enters $(\zeta_{i,n})^2$.

Proof. (i) First, an application of Mackey's formula reveals that Λ_i is the sum of two distinct irreducible characters of $G_2 = \mathrm{SU}_n(q)$. Clearly, $[\Lambda_i, 1_{G_2}] = 0$. By Proposition 4.5, Λ_i enters $(\zeta_n)^2 = \omega|_{G_2}$, so

$$\Lambda_i = C^\circ_{\beta_1} + C^\circ_{\beta_2}$$

for some $\beta_1 \neq \beta_2 \in \mathrm{Irr}(S_2)$. Next,

$$\Lambda_i(1) = (q^n-(-1)^n)(q^{n-1}+(-1)^n)/(q^2-1),$$

so $\beta_1, \beta_2 \neq \chi_{q+1}^{(t)}$, see Table I.

By Proposition 4.4, at least one of $\gamma_j := C^\circ_{\beta_j}$, $j = 1, 2$, is an irreducible constituent of

$$(\zeta_{i,n})^2 = D_{\lambda_{i,i}}|_{G_2},$$

see (4.7.2). As $\gamma_j \neq 1_{G_2}$, by Lemma 4.6 and Corollary 4.8 we have

$$[D_{\lambda_{i,i}}|_{G_2}, \gamma_j]_{G_2} = [\lambda_{i,i}, E_{\gamma_j}|_{S_1}]_{S_1} = [\lambda_{i,i}, \beta_j|_{S_1}]_{S_1}.$$

We have shown that $C^\circ_{\beta_j}$, is an irreducible constituent of $(\zeta_{i,n})^2$ precisely when $\lambda_{i,i}$ is an irreducible constituent of $\beta_j|_{S_1}$.

(ii) As in the proof of Proposition 4.4, let τ be an element of $\mathbb{F}_{q^{4k-2}}^{\times}$ of order $q^{2k-1}+1$ chosen such that $\tau^{(q^{2k-1}+1)/(q+1)} = \rho$. Then we fix an element $g \in L_1$ such that $g(e_1) = \sigma e_1$, $g(f_1) = \sigma^{-q} f_1$, and g is conjugate to

$$\mathrm{diag}(\sigma, \sigma^{-q}, \tau, \tau^{-q}, \tau^{q^2}, \dots, \tau^{(-q)^{2k-2}})$$

over $\overline{\mathbb{F}}_{q^2}$. By [Zs] there is a prime divisor ℓ of $q^{4k-2}-1$ that does not divide $\prod_{j=1}^{4k-3}(q^j - 1)$. In particular, ℓ divides $|\tau|$. It follows that σ and σ^{-q} are the only eigenvalues of g that belong to $\mathbb{F}_{q^2}$.

Assume in addition that $q > 2$; in particular, $\sigma \neq \sigma^{-q}$. Then, $\langle e_1 \rangle_{\mathbb{F}_{q^2}}$ and $\langle f_1 \rangle_{\mathbb{F}_{q^2}}$ are the only two g-invariant isotropic 1-spaces in W, and so

$$\Lambda_i(g) = 2\boldsymbol{\rho}^{-i}. \qquad (4.9.1)$$

Next, for any $x \in S_2 = \mathrm{GU}_2(q)$, $\omega(gx) = 1$, unless x has, at least one, and therefore both, of σ^{-1} and σ^q as its eigenvalues. In this exceptional case, x belongs to class $C_4^{(-1)}$ in the notation of [E], and $\omega(gx) = q^2$. It follows from Lemma 4.6 that

$$C^{\circ}_{\alpha}(g) = \begin{cases} \boldsymbol{\rho}^{-t}, & \alpha = \chi_1^{(t)},\ 0 < t \le q, \\ 2, & \alpha = \chi_1^{(0)}, \\ \boldsymbol{\rho}^{-t}, & \alpha = \chi_q^{(t)},\ 0 < t \le q, \\ 0, & \alpha = \chi_q^{(0)}, \\ 0, & \alpha = \chi_{q-1}^{(t,u)},\ 0 \le t, u \le q. \end{cases}$$

Together with (4.9.1), this readily implies that $\{\beta_1, \beta_2\} = \{\chi_1^{(i)}, \chi_q^{(i)}\}$. Note that $\chi_1^{(i)}|_{S_1} = \lambda_{i,i}$, but $\chi_q^{(i)}|_{S_1}$ does not contain $\lambda_{i,i}$, so we are done.

(iii) Now we consider the case $q = 2$. As shown in (i), we may assume that $\beta_1|_{S_1}$ contains $\lambda_{i,i}$. It follows that $\beta_1 \in \{\chi_1^{(i)}, \chi_{q-1}^{(2i,0)}\}$. However degree consideration using Table I rules out $\chi_{q-1}^{(2i,0)}$ and shows that $\beta_1 = \chi_1^{(i)}$. Again by degree consideration we now see that $\beta_2 = \chi_q^{(t)}$ for some $t \in \{1, 2\}$. Furthermore, g fixes exactly three isotropic 1-spaces in W (namely, the ones spanned by e_1, f_1, and $e_1 + f_1$), so $\Lambda_i(g) = 3\boldsymbol{\rho}^{-i}$. Arguing as in (ii), we see that

$$C^{\circ}_{\alpha}(g) = \begin{cases} \boldsymbol{\rho}^{-t}, & \alpha = \chi_1^{(t)},\ 0 < t \le q, \\ 2, & \alpha = \chi_1^{(0)}, \\ 2\boldsymbol{\rho}^{-t}, & \alpha = \chi_q^{(t)},\ 0 < t \le q, \\ 0, & \alpha = \chi_q^{(0)}. \end{cases}$$

Hence $\beta_2 = \chi_q^{(i)}$, and we are done since $\chi_q^{(i)}|_{S_1}$ does not contain $\lambda_{i,i}$. □

We will now work with three new dual pairs. First, we consider the dual pair $G_3 \times S_3$ inside $\Gamma := \mathrm{GU}_{2kn}(q)$, where $S_3 = \mathrm{GU}_{2k}(q)$ and $G_3 = \mathrm{SU}_n(q)$, and $\omega = \zeta_{2nk} = \zeta_{2nk,q}$. More precisely, we view S_3 as $\mathrm{GU}(U)$, where $U = \langle v_1, \dots, v_{2k} \rangle_{\mathbb{F}_{q^2}}$ is endowed with the Hermitian form $\circ$, with an orthonormal basis $(v_1,\ldots,v_{2k})$. Next, $G_3=\mathrm{SU}_n(q)$ is $\mathrm{SU}(W)$, where $W=\mathbb{F}_{q^2}^n$ is endowed with the Hermitian form $\circ$ defined in (4.0.1). Now we consider $V=U\otimes_{\mathbb{F}_{q^2}}W$ with the Hermitian form $\cdot$ defined via

$$(u\otimes w)\circ(u'\otimes w')=(u\circ u')(w\circ w')$$

for $u\in U$ and $w\in W$. The action of $G_3\times S_3$ on V induces a homomorphism $G_3\times S_3\to\Gamma:=\mathrm{GU}(V)$.

Now V is the orthogonal sum $\oplus_{i=1}^{2k}V_i$, where $V_i:=v_i\otimes W$. This gives us a subgroup

$$G_1:=\mathrm{SU}(V_1)\times\mathrm{SU}(V_2)\times\ldots\times\mathrm{SU}(V_{2k})\cong\mathrm{SU}_n(q)^{2k}$$

of Γ that contains (the image of) G_3. In fact, G_3 embeds diagonally in G_1: $g\mapsto\mathrm{diag}(g,g,\ldots,g)$. Next,

$$S_1:=\mathrm{GU}(\langle v_1\rangle_{\mathbb{F}_{q^2}})\times\mathrm{GU}(\langle v_2\rangle_{\mathbb{F}_{q^2}})\times\ldots\times\mathrm{GU}(\langle v_{2k}\rangle_{\mathbb{F}_{q^2}})\cong\mathrm{GU}_1(q)^{2k}$$

is just the non-split diagonal torus of S_3. In the above basis $(v_1,v_2,\ldots,v_{2k})$ of U and for $1\le i\le q$, we consider the character

$$\mu_i:\mathrm{diag}(\rho^{a_1},\rho^{a_2},\ldots,\rho^{a_{2k}})\mapsto\boldsymbol{\rho}^{i(\sum_{j=1}^{2k}a_j)}\tag{4.9.2}$$

of S_1.

Next, for each $1\le j\le k$ we embed one copy of $\mathrm{SU}(W)$ in

$$\mathrm{SU}(\langle v_{2j-1},v_{2j}\rangle_{\mathbb{F}_{q^2}}\otimes W)$$

(by letting it act only on W). This gives an embedding of $G_2:=\mathrm{SU}_n(q)^k$ in G_1 via

$$\mathrm{diag}(g_1,g_2,\ldots,g_k)\mapsto\mathrm{diag}(g_1,g_1,g_2,g_2,\ldots,g_k,g_k).$$

At the same times, G_3 embeds diagonally in G_2 via $g\mapsto\mathrm{diag}(g,g,\ldots,g)$. The action of G_2 is centralized by

$$S_2:=\mathrm{GU}(\langle v_1,v_2\rangle_{\mathbb{F}_{q^2}})\times\mathrm{GU}(\langle v_3,v_4\rangle_{\mathbb{F}_{q^2}})\times\ldots\times\mathrm{GU}(\langle v_{2k-1},v_{2k}\rangle_{\mathbb{F}_{q^2}})\cong\mathrm{GU}_2(q)^k.$$

Recall the characters C_α of $\mathrm{SU}_n(q)$ introduced in (4.7.3).

Proposition 4.10. *Suppose $n=2k+1\ge5$, $(n,q)\ne(5,2)$, and $0<i\le q$. Then both $(C_{\chi_1^{(i)}})^k$ and $(\zeta_{i,n})^{n-1}$ contain $\overline{\zeta}_{i,n}$.*

Proof. (i) First we decompose

$$\omega|_{G_3\times S_3}=\sum_{\gamma\in\mathrm{Irr}(G_3)}\gamma\otimes E_\gamma$$

for the dual pair $G_3\times S_3$. By Proposition 4.3, $\omega|_{G_3}=(\zeta_n)^{n-1}$ contains $\overline{\zeta}_{i,n}$ with multiplicity one. It follows that the G_3-character $E_{\overline{\zeta}_{i,n}}$ has degree 1, so there is some $0\le m=m_i\le q$ such that

$$E_{\overline{\zeta}_{i,n}}(X)=\boldsymbol{\rho}^{mt}$$

whenever $X \in \mathrm{GU}_{2k}(q)$ has determinant equal to ρ^t.

(ii) Next we decompose

$$\omega|_{S_2 \times G_2} = \sum_{\beta \in \mathrm{Irr}(S_2)} \beta \otimes F_\beta$$

for the dual pair $S_2 \times G_2$. Note by (4.7.3) that if

$$\beta = \beta_1 \otimes \beta_2 \otimes \ldots \otimes \beta_k,$$

then

$$F_\beta = C_{\beta_1} \otimes C_{\beta_2} \otimes \ldots \otimes C_{\beta_k}. \tag{4.10.1}$$

By Lemma 4.7,

$$[F_\beta|_{G_3}, \overline{\zeta}_{i,n}]_{G_3} = [\beta, E_{\overline{\zeta}_{i,n}}|_{S_2}]_{S_2}.$$

Since $E_{\overline{\zeta}_{i,n}}$ has degree 1, we see that $\overline{\zeta}_{i,n}$ is an irreducible constituent of $F_\beta|_{G_3}$ precisely when $\beta = E_{\overline{\zeta}_{i,n}}|_{S_2}$, that is when

$$\beta(X_1, X_2, \ldots, X_k) = \boldsymbol{\rho}^{m \sum_{j=1}^k t_j}$$

whenever $X_j \in \mathrm{GU}_2(q)$ has determinant equal to ρ^{t_j} for $1 \leq j \leq k$. In the notation of [E] we then have

$$\beta = \underbrace{\chi_1^{(m)} \otimes \chi_1^{(m)} \otimes \ldots \otimes \chi_1^{(m)}}_{k}. \tag{4.10.2}$$

(iii) Recall by Proposition 4.4 that Λ_i enters $(\zeta_n)^2$. It follows that $\Lambda_i^{\otimes k} = \underbrace{\Lambda_i \otimes \Lambda_i \otimes \ldots \otimes \Lambda_i}_{k}$ enters $\omega|_{G_2}$. Next, by Proposition 4.5, $\overline{\zeta}_{i,n}$ is an irreducible constituent of $(\Lambda_i)^k = \Lambda_i^{\otimes k}|_{G_3}$. Furthermore, by Proposition 4.9, $\Lambda_i = C_{\chi_1^{(i)}} + C_{\chi_q^{(i)}}$. Hence, using (4.10.1) we see that

$$\begin{aligned}
\Lambda_i^{\otimes k} &= \sum_{1 \leq j \leq k,\ \beta_j \in \{\chi_1^{(i)}, \chi_q^{(i)}\}} C_{\beta_1} \otimes C_{\beta_2} \otimes \ldots \otimes C_{\beta_k} \\
&= \sum_{1 \leq j \leq k,\ \beta_j \in \{\chi_1^{(i)}, \chi_q^{(i)}\}} F_{\beta_1 \otimes \beta_2 \otimes \ldots \otimes \beta_k}.
\end{aligned}$$

Applying the result (4.10.2) of (ii), we conclude that $m = i$ and $\overline{\zeta}_{i,n}$ is an irreducible constituent of

$$F_{\chi_1^{(m)} \otimes \chi_1^{(m)} \otimes \ldots \otimes \chi_1^{(m)}}|_{G_3} = (C_{\chi_1^{(i)}})^k.$$

(iv) The same argument as in (ii), but applied to the decomposition

$$\omega|_{S_1 \times G_1} = \sum_{\alpha \in \mathrm{Irr}(S_1)} \alpha \otimes D_\alpha$$

for the dual pair $S_1 \times G_1$ implies that $\overline{\zeta}_{i,n}$ is an irreducible constituent of $D_\alpha|_{G_3}$ precisely when $\alpha = E_{\overline{\zeta}_{i,n}}|_{S_1}$, that is when $\alpha = \mu_m$ as introduced in (4.9.2). As m was shown to be equal to i in (iii), we now have that $\overline{\zeta}_{i,n}$ is an irreducible constituent of

$$D_\alpha|_{G_3} = D_{\mu_i}|_{G_3} = (\zeta_{i,n})^{n-1}.$$

□

We can now prove the main result of this section:

Theorem 4.11. *Let q be a prime power and let $G = \mathrm{SU}_n(q)$ with $n = 2k+1 \geq 3$. Suppose in addition that $(n,q) \neq (3,2)$. Then $(\zeta_{i,n})^n$ contains 1_G with multiplicity exactly one if $1 \leq i \leq q$ and zero if $i = 0$.*

Proof. For $n = 3$, the statement was checked by A. Schaeffer Fry using the package Chevie. Likewise, the case $(n,q) = (5,2)$ was checked using the package GAP. So we may assume that $n \geq 5$ and $(n,q) \neq (5,2)$. Now for $i = 0$ the statement follows from Proposition 4.3. For $1 \leq i \leq q$ we have

$$[(\zeta_{i,n})^{n-1}, \overline{\zeta}_{i,n}]_G = [(\zeta_{i,n})^n, 1_G]$$

is at most 1 by Proposition 4.3 and at least 1 by Proposition 4.10. □

Theorem 4.11 means that the Weil representation of $\mathrm{SU}_n(q)$ affording the character $\zeta_{i,n}$ with $1 \leq i \leq q$ has a unique (up to scalar) polynomial invariant of degree n. It would be interesting to know what is the geometric significance of this polynomial invariant, and to find an explicit construction of it.

5. Moments of Weil representations of $\mathrm{SU}_4(q)$

Theorem 4.11 naturally brings up the question: what are the n-moments of Weil representations of $\mathrm{SU}_n(q)$ when $2|n$? Preliminary analysis indicates that the even-dimensional case does not behave as nicely as in the odd-dimensional case (particularly because real-valued characters usually have large even moments). We restrict ourselves to record the following result:

Theorem 5.1. *Consider the irreducible Weil characters $\zeta_{i,n}$, $0 \leq i \leq q$, of $G := \mathrm{SU}_n(q)$ as given in (2.0.2), and suppose $n = 4$. Then*

$$[(\zeta_{i,4})^4, 1_G] = \begin{cases} q+1, & i = 0, \\ q+2, & 2 \nmid q,\ i = (q+1)/2, \\ q-1, & 4|(q+1),\ i = (q+1)/4,\ 3(q+1)/4, \\ 1, & \textit{otherwise}. \end{cases}$$

Proof. (i) We will use the dual pairs $G_1 \times S_1 = \mathrm{SU}_n(q)^2 \times \mathrm{GU}_1(q)^2$ and $G_2 \times S_2 = \mathrm{SU}_n(q) \times \mathrm{GU}_2(q)$ as in (4.7.1). By [LBST, Proposition 6.3],

$$\begin{aligned}\omega|_{G_2 \times S_2} &= \sum_{\alpha \in \mathrm{Irr}(S_2)} C_\alpha \otimes \alpha = \sum_{\gamma \in \mathrm{Irr}(G_2)} \gamma \otimes E_\gamma \\ &= \sum_{\alpha \in \mathrm{Irr}(S_2)} C^\circ_\alpha \otimes \alpha + 1_{G_2} \otimes (\chi_1^{(0)} + \chi_q^{(0)})\end{aligned},$$

where $C^\circ_\alpha(1)$ are listed in Table I. The only new feature that arises in the case $n = 4$ is that, according to [LBST, Proposition 6.5],

(a) If $\alpha \neq \beta$, then $C^\circ_\alpha = C^\circ_\beta$ precisely when $\{\alpha, \beta\} = \{\chi_1^{(t)}, \chi_1^{(q+1-t)}\}$ for some $t \in \{1, 2, \dots, q\} \smallsetminus \{(q+1)/2\}$; and

(b) All C°_α are irreducible, except when $2 \nmid q$ and $\alpha = \chi_1^{(q+1)/2}$, in which case C°_α is a sum of two distinct irreducible characters (of degree $(q^2+1)(q^2-q+1)/2$).

Hence, instead of Corollary 4.8 now we have

$$E_\gamma = \begin{cases} \alpha, & \text{if } \gamma \text{ is an irreducible constituent} \\ & \text{of } C^\circ_\alpha \text{ for some } \alpha \in \mathrm{Irr}(\mathrm{GU}_2(q)), \\ \chi_1^{(0)} + \chi_q^{(0)}, & \text{if } \gamma = 1_{G_2}, \\ 0, & \text{otherwise.} \end{cases} \tag{5.1.1}$$

On the other hand,

$$\omega|_{G_1 \times S_1} = \sum_{\alpha \in \mathrm{Irr}(S_1)} D_\alpha \otimes \alpha,$$

where D_α is given in (4.7.2) for $\alpha = \lambda_{i,j} \in \mathrm{Irr}(\mathrm{GU}_1(q)^2)$. Applying Lemma 4.7 we then get

$$(\zeta_{i,4})^2|_{\mathrm{SU}_4(q)} = D_{\lambda_{i,i}}|_{G_2} = \sum_{\gamma \in \mathrm{Irr}(G_2} [E_\gamma|_{\mathrm{GU}_1(q)^2}, \lambda_{i,i}]_{\mathrm{GU}_1(q)^2} \cdot \gamma. \tag{5.1.2}$$

Direct computations show for $\alpha \in \mathrm{Irr}(\mathrm{GU}_2(q))$ that

$$[\alpha|_{\mathrm{GU}_1(q)^2}, \lambda_{i,i}]_{\mathrm{GU}_1(q)^2} = \begin{cases} \delta_{t,i}, & \alpha = \chi_1^{(t)}, \\ \delta_{t,2i}, & \alpha = \chi_{q+1}^{(t)}, \\ \delta_{t+u,2i}, & \alpha = \chi_{q-1}^{(t,u)}, \\ \delta_{t,i+(q+1)/2}, & \alpha = \chi_q^{(t)},\ 2 \nmid q, \\ 0, & \alpha = \chi_q^{(t)},\ 2|q, \end{cases} \tag{5.1.3}$$

and $\delta_{i,j}$ is defined to be 1 if $i \equiv j (\bmod\, q+1)$ and 0 otherwise. Recall that in the notation for $\alpha \in \mathrm{Irr}(\mathrm{GU}_2(q))$, the superscripts are viewed as elements of $\mathbb{Z}/(q+1)\mathbb{Z}$ if $\alpha(1) \leq q$, and as elements of $\mathbb{Z}/(q^2-1)\mathbb{Z}$ if $\alpha(1) = q+1$. Moreover, $\chi_{q-1}^{(t,u)} = \chi_{q-1}^{(u,t)}$ and $\chi_{q+1}^{(t)} = \chi_{q+1}^{(-tq)}$.

(ii) Consider the case $2|q$. Then (5.1.1)–(5.1.3) imply that

$$(\zeta_{0,4})^2 = 1_G + C^\circ_{\chi_1^{(0)}} + \sum_{1\le t\le q/2} C^\circ_{\chi_{q-1}^{(t,-t)}} + \sum_{1\le s\le (q-2)/2} C^\circ_{\chi_{q+1}^{(s(q+1))}}.$$

As $\zeta_{0,4}$ is real-valued, it follows that $[(\zeta_{0,4})^4, 1_G]_G = q+1$.

Likewise, if $i \neq 0$, then the irreducible summands of $(\zeta_{i,4})^2$ are $C^\circ_{\chi_1^{(i)}}$, $C^\circ_{\chi_{q-1}^{(t,2i-t)}}$ with $t \neq i$, and $C^\circ_{\chi_{q+1}^{(s)}}$ with $s \equiv 2i (\mathrm{mod}\, q+1)$ (and $s \not\equiv 0 (\mathrm{mod}\, q-1)$); all with multiplicity one. It follows that the only common irreducible constituent of $(\zeta_{i,4})^2$ and $(\overline{\zeta}_{i,4})^2 = (\zeta_{q+1-i,4})^2$ is $C^\circ_{\chi_1^{(i)}} = C^\circ_{\chi_1^{(q+1-i)}}$, cf. (a) above. Thus $[(\zeta_{i,4})^4, 1_G]_G = 1$. In fact, this argument also applies to the case where $2 \nmid q$ and $(q+1) \nmid 4i$, where there is an extra irreducible summand $C^\circ_{\chi_q^{(i+(q+1)/2)}}$ (also with multiplicity 1) in $(\zeta_{i,4})^2$.

(iii) Assume now that $2 \nmid q$. Then (5.1.1)–(5.1.3) imply that

$$(\zeta_{0,4})^2 = 1_G + C^\circ_{\chi_1^{(0)}} + \sum_{1\le t\le \frac{q-1}{2}} C^\circ_{\chi_{q-1}^{(t,-t)}} + C^\circ_{\chi_q^{(\frac{q+1}{2})}} + \sum_{1\le s\le \frac{q-3}{2}} C^\circ_{\chi_{q+1}^{(s(q+1))}},$$

yielding $[(\zeta_{0,4})^4, 1_G]_G = q+1$. Likewise,

$$(\zeta_{\frac{q+1}{2},4})^2 = 1_G + C^\circ_{\chi_1^{(\frac{q+1}{2})}} + \sum_{1\le t\le \frac{q-1}{2}} C^\circ_{\chi_{q-1}^{(t,-t)}} + C^\circ_{\chi_q^{(0)}} + \sum_{1\le s\le \frac{q-3}{2}} C^\circ_{\chi_{q+1}^{(s(q+1))}}.$$

Since $\zeta_{\frac{q+1}{2},4}$ is real-valued and $C^\circ_{\chi_1^{(\frac{q+1}{2})}}$ is the sum of two distinct irreducible summands, $[(\zeta_{\frac{q+1}{2},4})^4, 1_G]_G = q+2$.

Finally, the irreducible summands of $(\zeta_{\frac{q+1}{4},4})^2$ are $C^\circ_{\chi_q^{(-\frac{q+1}{4})}}$, $C^\circ_{\chi_1^{(\frac{q+1}{4})}}$, $C^\circ_{\chi_{q-1}^{(t,\frac{q+1}{2}-t)}}$ with $t \neq \pm(q+1)/4$, and $C^\circ_{\chi_{q+1}^{(2s+1)(q+1)/2}}$; all with multiplicity one. As mentioned in (a), $C^\circ_{\chi_1^{(\frac{q+1}{4})}} = C^\circ_{\chi_1^{-(\frac{q+1}{4})}}$. Thus all of these characters, except for the first one, are common irreducible summands between $(\zeta_{\frac{q+1}{4},4})^2$ and $(\overline{\zeta}_{\frac{q+1}{4},4})^2 = (\zeta_{\frac{3(q+1)}{4},4})^2$. It follows that $[(\zeta_{\frac{q+1}{4},4})^4, 1_G]_G = q-1$. □

References

[As] Aschbacher, M., Maximal subgroups of classical groups, On the maximal subgroups of the finite classical groups, Invent. Math. 76 (1984), 469–514.

[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.

[BHR] Bray, J. N., Holt, D. F., and Roney-Dougal, C. M., The maximal subgroups of the low-dimensional finite classical groups. With a foreword by Martin Liebeck. London Mathematical Society Lecture Note Series, **407**, 2013.

[Cam] Cameron, P. J., Finite permutation groups and finite simple groups, *Bull. Lond. Math. Soc.* **13** (1981), 1–22.

[C-R] Curtis, C. W. and Reiner, I., Representation theory of finite groups and associative algebras, Interscience Publishers, New York 1962, xiv+689 pp.

[De-Weil II] Deligne, P., La conjecture de Weil II, Pub. Math. I.H.E.S. 52 (1981), 313-428.

[DM] Digne, F. and Michel, J., Representations of Finite Groups of Lie Type, London Mathematical Society Student Texts 21, Cambridge University Press, 1991.

[E] V. Ennola, On the characters of the finite unitary groups, Ann. Acad. Scient. Fenn. A I, no. 323 (1963).

[F2] Feit, W., On large Zsigmondy primes, *Proc. Amer. Math. Soc.* **102** (1988), 28–36.

[FH] W. Fulton and J. Harris, *Representation Theory*, Springer-Verlag, New York, 1991.

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

[GLS] Gorenstein, D., Lyons, R., and Solomon, R.M., The Classification of the Finite Simple Groups, Number 3. Part I. Chapter A, volume 40 of Mathematical Surveys and Monographs, American Mathematical Society, Providence, RI, 1998.

[Gross] Gross, B. H., Rigid local systems on $\mathbb{G}_m$ with finite monodromy. Adv. Math. 224 (2010), no. 6, 2531-2543.

[Gro-FL] Grothendieck, A., Formule de Lefschetz et rationalité des fonctions L, Seminaire Bourbaki 1964-65, Exposé 279, reprinted in Dix Exposés sur la cohomologie des schémas, North-Holland, 1968.

[GKT] Guralnick, R. M., Katz, N., and Tiep, P. H., Rigid local systems and alternating groups, (submitted).

[GMST] Guralnick, R. M., Magaard, K., Saxl, J., and Tiep, P. H., Cross characteristic representations of symplectic groups and unitary groups, *J. Algebra* **257** (2002), 291–347.

[GPPS] Guralnick, R. M., Penttila, T., Praeger, C., Saxl, J., Linear groups with orders having certain large prime divisors, *Proc. London Math. Soc.* **78** (1999), 167–214.

[GT] Guranick, R. M. and Tiep, P. H., Symmetric powers and a conjecture of Kollar and Larsen, Invent. Math. 174 (2008), 505–554.

[Ho] Howe, R., Another look at the local θ-correspondence for an unramified dual pair. Festschrift in honor of I. I. Piatetski-Shapiro on the occasion of his sixtieth birthday, Part I (Ramat Aviv, 1989), 93–124, Israel Math. Conf. Proc., 2, Weizmann, Jerusalem, 1990.

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

[Ka-GKM] Katz, N., Gauss Sums, Kloosterman Sums, and Monodromy Groups, Annals of Mathematics Studies, 116. Princeton Univ. Press, Princeton, NJ, 1988. ix+246 pp.

[Ka-MMP] Katz, N.,Moments, Monodromy, and Perversity. Annals of Mathematics Studies, 159. Princeton University Press, Princeton, NJ, 2005. viii+475 pp.

[Ka-NG2] Katz, N., Notes on G_2, determinants, and equidistribution, Finite Felds and their Applications 10 (2004), 221-269.

[Ka-PES] Katz, N., Perversity and Exponential Sums,in Algebraic Number Theory - in honor of K. Iwasawa, Advanced Studies in Pure Mathematics 17, 1989, 209-259.

[Ka-RLS] Katz, N., Rigid Local Systems. Annals of Mathematics Studies, 139. Princeton University Press, Princeton, NJ, 1996. viii+223 pp.

[Ka-RLSFM] Katz, N., Rigid local systems on $\mathbb{A}^1$ with finite monodromy. preprint available at www.math.princeton.edu/~nmk/gpconj87.pdf.

[Ka-Sar] 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.

[KT1] Katz, N., with an Appendix by Tiep, P.H., Rigid local systems on $\mathbb{A}^1$ with finite monodromy, (submitted).

[KT2] Katz, N., and Tiep, P.H., Rigid local systems and finite symplectic groups, (submitted).

[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.

[Ku] S. Kudla, Seesaw dual reductive pairs, in: '*Automorphic Forms of Several Variables*', Taniguchi Symposium, Katata, 1983, Birkhäuser, Boston, 1983, pp. 244–268.

[LBST] Liebeck, M. W., O'Brien, E., Shalev, A., and Tiep, P. H., The Ore conjecture, *J. Eur. Math. Soc.* **12** (2010), 939–1008

[LS] Liebeck, M. W. and Seitz, G. M. On the subgroup structure of classical groups, Invent. Math. 134 (1998), 427–453.

[Lu] Lübeck, F., Character degrees and their multiplicities for some groups of Lie type of rank < 9, http://www.math.rwth-aachen.de/~Frank.Luebeck/chev/DegMult/index.html.

[Pa] Panyushev, D. I., Weight Multiplicity Free Representations, g-Endomorphism Algebras, and Dynkin Polynomials, J. London Math. Soc. 69 (2004), 273–290.

[Ra] Rasala, R., On the minimal degrees of characters of S_n, J. Algebra 45 (1977), 132-181.

[Ray] Raynaud, M. Revêtements de la droite affine en caractéristique p > 0 et conjecture d'Abhyankar. Invent. Math. 116 (1994), no. 1-3, 425-462.

[ST] Sin, P., and Tiep, P. H., Rank 3 permutation modules for finite classical groups, *J. Algebra* **291** (2005), 551–606.

[T] Tiep, P. H., Low dimensional representations of finite quasisimple groups, Proceedings of the London Math. Soc. Symposium "Groups, Geometries, and Combinatorics", Durham, July 2001, A. A. Ivanov et al eds., World Scientific, 2003, N. J. 277–294.

[TZ1] Tiep, P. H. and Zalesskii, A. E., Minimal characters of the finite classical groups, Comm. Algebra 24 (1996), 2093–2167.

[TZ2] Tiep, P. H. and Zalesskii, A. E., Some characterizations of the Weil representations of the symplectic and unitary groups, *J. Algebra* **192** (1997), 130–165.

[Zs] Zsigmondy, K., Zur Theorie der Potenzreste, *Monatsh. Math. Phys.* **3** (1892), 265–284.

Department of Mathematics, Princeton University, Princeton, NJ 08544
E-mail address: nmk@math.princeton.edu

Department of Mathematics, Rutgers University, Piscataway, NJ 08854
E-mail address: tiep@math.rutgers.edu