J. Aust. Math. Soc. **117** (2024), 130–148
doi:10.1017/S1446788724000016

THE $(2, 3)$-GENERATION OF THE FINITE SIMPLE ODD-DIMENSIONAL ORTHOGONAL GROUPS

MARCO ANTONIO PELLEGRINI and MARIA CHIARA TAMBURINI BELLANI

(Received 1 July 2023; accepted 14 January 2024; first published online 28 February 2024)

Communicated by Michael Giudici

Abstract

The complete classification of the finite simple groups that are $(2, 3)$-generated is a problem which is still open only for orthogonal groups. Here, we construct $(2, 3)$-generators for the finite odd-dimensional orthogonal groups $\Omega_{2k+1}(q)$, $k \geq 4$. As a byproduct, we also obtain $(2, 3)$-generators for $\Omega^+_{4k}(q)$ with $k \geq 3$ and q odd, and for $\Omega^{\pm}_{4k+2}(q)$ with $k \geq 4$ and $q \equiv \pm 1 \pmod 4$.

2020 *Mathematics subject classification*: primary 20G40; secondary 20F05.

Keywords and phrases: orthogonal group, simple group, generation.

1. Introduction

A group is said to be $(2, 3)$-generated if it can be generated by an involution and an element of order 3, equivalently if it is an epimorphic image of $C_2 * C_3 \cong \mathrm{PSL}_2(\mathbb{Z})$. In 1996 (see [6]), it was shown that the symplectic groups $\mathrm{PSp}_4(q)$, with $q = 2^f, 3^f$, are not $(2, 3)$-generated and that, apart from the members of these two infinite families and a finite number of undetermined exceptions, the finite simple classical groups, defined over the Galois field $\mathbb{F}_q$, are $(2, 3)$-generated. Since then, many authors contributed to a constructive solution of the $(2, 3)$-generation problem of these groups (for example, see [13, 14]). As a consequence, the list $\mathcal{L}$ of the known exceptions consists now of the following ten groups: $\mathrm{PSL}_2(9)$, $\mathrm{PSL}_3(4)$, $\mathrm{PSL}_4(2)$, $\mathrm{PSU}_3(3^2)$, $\mathrm{PSU}_3(5^2)$, $\mathrm{PSU}_4(2^2) \cong \mathrm{PSp}_4(3)$, $\mathrm{PSU}_4(3^2)$, $\mathrm{PSU}_5(2^2)$, $\mathrm{P}\Omega^+_8(2)$ and $\mathrm{P}\Omega^+_8(3)$. This list is complete for linear, unitary and symplectic groups, as shown in [8–10].

In [11], we proved that the finite simple 8-dimensional orthogonal groups are $(2, 3)$-generated, with the exceptions of $\mathrm{P}\Omega^+_8(2)$ and $\mathrm{P}\Omega^+_8(3)$ found by Vsemirnov [16]. In this paper, we consider orthogonal groups of dimension $n \geq 9$ and prove the following constructive result.

THEOREM 1.1. *Assume q is odd. The following orthogonal groups are $(2,3)$-generated:*

(i) $\Omega_{2k+1}(q)$ *with* $k \geq 4$;
(ii) $\Omega^+_{4k}(q)$ *with* $k \geq 3$;
(iii) $\Omega^+_{4k+2}(q)$ *with* $k \geq 4$ *and* $q \equiv 1 \pmod 4$;
(iv) $\Omega^-_{4k+2}(q)$ *with* $k \geq 4$ *and* $q \equiv 3 \pmod 4$.

We recall that the $(2,3)$-generation of $\Omega_5(q) \cong \mathrm{PSp}_4(q)$, when $\gcd(q,6) = 1$, was proved in [2] (see also [12]). Notice that the groups $\Omega_5(3^f)$ are not $(2,3)$-generated, but they are $(2,5)$-generated (see [4]). In [7], it was proved that the groups $\Omega_7(q)$ are $(2,3)$-generated for all odd q. As a consequence of all this, the constructive $(2,3)$-generation problem for the finite simple classical groups remains open only for the following orthogonal groups:

(i) $\mathrm{P}\Omega^\pm_{2k}(q)$ with $k \geq 5$ and q even;
(ii) $\mathrm{P}\Omega^\pm_{10}(q)$, $\mathrm{P}\Omega^\pm_{14}(q)$, q odd;
(iii) $\mathrm{P}\Omega^-_{4k}(q)$ with $k \geq 3$ and q odd;
(iv) $\mathrm{P}\Omega^+_{4k+2}(q)$ with $k \geq 4$ and $q \equiv 3 \pmod 4$;
(v) $\mathrm{P}\Omega^-_{4k+2}(q)$ with $k \geq 4$ and $q \equiv 1 \pmod 4$.

In our proof of Theorem 1.1, the cases $n \in \{9, 11, 13, 17\}$ are dealt with in Section 3, where we use slightly different generators to make the proofs more efficient. For the general case, the generators are given in Section 4. The corresponding proofs are in Section 5 for $n \in \{15, 18, 19\}$ or $n \geq 21$ and in Section 6 for $n \in \{12, 16, 20\}$.

2. Preliminary results

Let $\mathbb{F}_q$ be the Galois field of order $q = p^f$, a power of the prime $p > 2$, and let $\mathbb{F}$ be the algebraic closure of the field $\mathbb{F}_p$. We make $\mathrm{GL}_n(\mathbb{F})$ act on the left on $V = \mathbb{F}^n$, whose canonical basis is $\mathscr{C} = \{e_1, e_2, \ldots, e_n\}$.

Up to isometry, there are two nondegenerate quadratic forms on $\mathbb{F}_q^n$. If n is even, these two forms are not similar: we say that the quadratic form has sign $+$ if the dimension of any maximal totally singular subspace is $n/2$; it has sign $-$ if the dimension of such a space is $n/2 - 1$. The corresponding isometry groups are denoted by $\mathrm{O}^+_n(q)$ and $\mathrm{O}^-_n(q)$. If n is odd, the two quadratic forms are similar. Hence, the corresponding isometry groups are isomorphic and are denoted by $\mathrm{O}^\circ_n(q)$, or simply by $\mathrm{O}_n(q)$. In short, we write $\mathrm{O}^\epsilon_n(q)$, where $\epsilon = \circ$ if n is odd, $\epsilon = +$ or $\epsilon = -$ if n is even.

If J is the Gram matrix of the symmetric bilinear form β associated to a nondegenerate quadratic form Q on $\mathbb{F}_q^n$,

$$\beta(v,w) = v^{\mathsf{T}} J w \quad \text{and} \quad 2Q(v) = \beta(v,v) \quad \text{for all } v, w \in \mathbb{F}_q^n.$$

In particular, since q is assumed to be odd, the form Q is determined by β, that is, by J. When n is even, the isometry group of J is $\mathrm{O}^+_n(q)$ if either $\det(J)$ is a square in $\mathbb{F}_q^*$ and $n(q-1)/4$ is even, or $\det(J)$ is a nonsquare and $n(q-1)/4$ is odd; it is $\mathrm{O}^-_n(q)$ otherwise (see [1, Proposition 1.5.42]).

https://doi.org/10.1017/S1446788724000016 Published online by Cambridge University Press

The group $\Omega_n^\epsilon(q)$ is the derived subgroup of $\mathrm{O}_n^\epsilon(q)$ and has index 2 in $\mathrm{SO}_n^\epsilon(q)$, the subgroup of $\mathrm{O}_n^\epsilon(q)$ consisting of matrices of determinant 1. Alternatively, $\Omega_n^\epsilon(q)$ consists of the elements in $\mathrm{SO}_n^\epsilon(q)$ with spinor norm in $(\mathbb{F}_q^*)^2$. We recall that the spinor norm $\theta : \mathrm{O}_n^\epsilon(q) \to \mathbb{F}_q^*/(\mathbb{F}_q^*)^2$ is a homomorphism. For any nonsingular $v \in \mathbb{F}_q^n$, the reflection r_v, of centre $\langle v\rangle$, acts as $w \mapsto w - Q(v)^{-1}\beta(w, v)v$ for all $w \in V$. Moreover, $\theta(r_v) = Q(v)(\mathbb{F}_q^*)^2$ (see [15, pages 145, 163 and 164]).

Given an eigenvalue λ of a matrix $g \in \mathrm{GL}_n(\mathbb{F})$, write $V_\lambda(g)$ for the corresponding eigenspace. The characteristic polynomial of g is denoted by $\chi_g(t)$. Let $\omega \in \mathbb{F}$ be a primitive cube root of 1.

Lemma 2.1. *Let H be a subgroup of $\mathrm{GL}_n(\mathbb{F})$ and U be a proper H-invariant subspace. Suppose that $g \in H$ has the eigenvalue $\lambda \in \mathbb{F}$. If the restriction $g_{|U}$ does not have the eigenvalue λ, then there exists an H^{T}-invariant subspace $\overline{U}$, with $\dim(\overline{U}) = n - \dim(U)$, such that $V_\lambda(g^{\mathsf{T}}) \leq \overline{U}$.*

Proof. There exists a nonsingular matrix P such that

$$P^{-1}HP = \left\{\begin{pmatrix} A_h & B_h \\ 0 & C_h \end{pmatrix} \mid h \in H\right\}, \quad P^{\mathsf{T}}H^{\mathsf{T}}P^{-\mathsf{T}} = \left\{\begin{pmatrix} A_h^{\mathsf{T}} & 0 \\ B_h^{\mathsf{T}} & C_h^{\mathsf{T}} \end{pmatrix} \mid h \in H\right\}.$$

Set $A = A_g$, $B = B_g$, $C = C_g$ and $k = \dim(U)$. Under our assumption, $A \in \mathrm{GL}_k(\mathbb{F})$ does not have the eigenvalue λ. Hence, the same is true for A^{T}. So, imposing

$$\begin{pmatrix} A^{\mathsf{T}} & 0 \\ B^{\mathsf{T}} & C^{\mathsf{T}} \end{pmatrix}\begin{pmatrix} w \\ \overline{w} \end{pmatrix} = \begin{pmatrix} A^{\mathsf{T}}w \\ B^{\mathsf{T}}w + C^{\mathsf{T}}\overline{w} \end{pmatrix} = \begin{pmatrix} \lambda w \\ \lambda\overline{w} \end{pmatrix}, \quad w \in \mathbb{F}^k,\ \overline{w} \in \mathbb{F}^{n-k},$$

we get $w = 0$ and

$$V_\lambda(P^{\mathsf{T}}g^{\mathsf{T}}P^{-\mathsf{T}}) = \left\{\begin{pmatrix} 0 \\ \overline{w} \end{pmatrix} \mid C^{\mathsf{T}}\overline{w} = \lambda\overline{w}\right\} \leq \overline{E} = \langle e_i \mid k+1 \leq i \leq n\rangle.$$

Set $\overline{U} = P^{-\mathsf{T}}\overline{E}$. Since $\overline{E}$ is invariant under $P^{\mathsf{T}}H^{\mathsf{T}}P^{-\mathsf{T}}$, we get that $\overline{U}$ is H^{T}-invariant. From $V_\lambda(g^{\mathsf{T}}) = P^{-\mathsf{T}}V_\lambda(P^{\mathsf{T}}g^{\mathsf{T}}P^{-\mathsf{T}})$, it follows that $V_\lambda(g^{\mathsf{T}}) \leq \overline{U}$. □

Corollary 2.2. *Let H be a subgroup of $\mathrm{GL}_n(\mathbb{F})$ and U be a proper H-invariant subspace. Suppose that there exists $J \in \mathrm{GL}_n(\mathbb{F})$ such that $h^{\mathsf{T}}Jh = J$ for all $h \in H$. If $g \in H$ has the eigenvalue $\lambda \in \mathbb{F}$, then*

$$J^{-1}V_\lambda(g^{\mathsf{T}}) = V_{\lambda^{-1}}(g).$$

Also, if $g_{|U}$ does not have the eigenvalue λ, then there exists an H-invariant subspace W, with $\dim(W) = n - \dim(U)$, such that $V_{\lambda^{-1}}(g) \leq W$.

In particular, for $\lambda = \lambda^{-1}$ (that is, $\lambda = \pm 1$), we may assume that $g_{|U}$ has the eigenvalue λ.

Proof. From $g^{\mathsf{T}}Jg = J$, we get $g(J^{-1}\overline{s}) = J^{-1}g^{-\mathsf{T}}\overline{s} = \lambda^{-1}(J^{-1}\overline{s})$ for all $\overline{s} \in V_\lambda(g^{\mathsf{T}})$. It follows that $J^{-1}V_\lambda(g^{\mathsf{T}}) \leq V_{\lambda^{-1}}(g)$. However, take $v \in V_{\lambda^{-1}}(g)$. Then, $g^{\mathsf{T}}Jv = Jg^{-1}v = \lambda Jv$ gives $Jv \in V_\lambda(g^{\mathsf{T}})$, whence $V_{\lambda^{-1}}(g) \leq J^{-1}V_\lambda(g^{\mathsf{T}})$.

https://doi.org/10.1017/S1446788724000016 Published online by Cambridge University Press

If $g_{|U}$ does not have the eigenvalue λ, we apply Lemma 2.1: so, there exists an H^{T}-invariant subspace $\overline{U}$, with $\dim(\overline{U}) = n - \dim(U)$, such that $V_\lambda(g^{\mathsf{T}}) \leq \overline{U}$. Set $W = J^{-1}\overline{U}$. For any $h \in H$, we have $hW = h(J^{-1}\overline{U}) = J^{-1}h^{-\mathsf{T}}\overline{U} = J^{-1}\overline{U} = W$. Hence, W is H-invariant and $\dim(W) = \dim(\overline{U}) = n - \dim(U)$. Finally, $V_{\lambda^{-1}}(g) = J^{-1}V_\lambda(g^{\mathsf{T}}) \leq J^{-1}\overline{U} = W$. □

To prove our Theorem 1.1, we define two elements x, y of respective orders 2 and 3, where $y \in \Omega_n^\epsilon(q)$ and x depends on some parameter $a \in \mathbb{F}_q^*$. Our aim is to find suitable conditions on a such that $x \in \Omega_n^\epsilon(q)$ and the subgroup $H = \langle x, y\rangle$ is not contained in any maximal subgroup M of $\Omega_n^\epsilon(q)$.

The maximal subgroups of classical groups, described in [1, 5], belong to eight classes $\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_8$, and a further class $\mathcal{S}$. Note that, for orthogonal groups, the class $\mathcal{C}_8$ is always empty. Those which are relevant in our results can be roughly described as follows (see [5, Table 1.2.A]):

- groups that are reducible over $\mathbb{F}$ (classes $\mathcal{C}_1$ and $\mathcal{C}_3$);
- *imprimitive* groups, that is, stabilizers of decompositions $\mathbb{F}_q^n = \oplus_{i=1}^t W_i$, where $\dim(W_i) = n/t$ (class $\mathcal{C}_2$). When $t = n$, they are also called *monomial*;
- stabilizers of subfields of $\mathbb{F}_q$ of prime index (class $\mathcal{C}_5$). They are conjugate to subgroups of $\mathrm{GL}_n(q_0)$, where $q = q_0^r$ with r prime.

To understand these groups, it is also necessary to know the representations of classical groups in higher dimensions, where they may fix nondegenerate forms. In particular, we need (for instance, in Lemma 3.5) the representation $\psi : \mathrm{GL}_2(q) \to \mathrm{GL}_3(q)$ arising from the action of $\mathrm{GL}_2(q)$ on the space of homogeneous polynomials of degree 2 in two variables over $\mathbb{F}_q$, namely

$$\psi\left(\begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix}\right) = \begin{pmatrix} b_1^2 & b_1b_2 & b_2^2 \\ 2b_1b_3 & b_1b_4 + b_2b_3 & 2b_2b_4 \\ b_3^2 & b_3b_4 & b_4^2 \end{pmatrix}. \tag{2-1}$$

Note that $\mathrm{Im}(\psi)$ preserves the symmetric form $\left(\begin{smallmatrix} 0 & 0 & 1 \\ 0 & -1/2 & 0 \\ 1 & 0 & 0 \end{smallmatrix}\right)$ whenever $b_1b_4 - b_2b_3 = \pm 1$.

Finally, we recall some well-known facts (for example, see [5, page 185]). Let $\mathrm{Sym}(\ell)$ be the subgroup of $\mathrm{GL}_\ell(\mathbb{F})$ consisting of the permutation matrices. Clearly, $\mathrm{Sym}(\ell)$ preserves the bilinear form defined by I_ℓ. Moreover, it fixes the vector $u = \sum_{i=1}^{\ell} e_i$ and the subspace $u^\perp$.

If $p \nmid \ell$, then u is not isotropic, whence $\mathbb{F}^\ell = u^\perp \perp \langle u\rangle$. The restriction of $\mathrm{Sym}(\ell)$ to the subspace $u^\perp$ provides a representation of $\mathrm{Sym}(\ell)$ of degree $\ell - 1$. The Jordan canonical form of any $\sigma \in \mathrm{Sym}(\ell)$ is obtained from the Jordan form of $\sigma_{|u^\perp}$, adding a unique block $(\,1\,)$.

If $p \mid \ell$, then $u \in u^\perp$. Set $\overline{W} = \langle e_1 - e_{i+1} \mid 1 \leq i \leq \ell - 2\rangle$. With respect to the decomposition $u^\perp = \overline{W} \oplus \langle u\rangle$, every $\sigma \in \mathrm{Sym}(\ell)$ has matrix

$$\begin{pmatrix} \sigma_{|\overline{W}} & 0 \\ v_\sigma^{\mathsf{T}} & 1 \end{pmatrix}, \quad \sigma_{|\overline{W}} \in \mathrm{GL}_{\ell-2}(p), \quad v_\sigma \in \mathbb{F}_p^{\ell-2}.$$

https://doi.org/10.1017/S1446788724000016 Published online by Cambridge University Press

$$\bar{x} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{2}{a} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \frac{a}{2} & 0 & 0 \end{pmatrix}, \quad \bar{y} = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -2 & 1 & 0 & -2 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -\frac{1}{2} & 0 & 0 \end{pmatrix}.$$

FIGURE 1. Generators of $\Omega_9(q)$.

The representation $\sigma \mapsto \sigma_{|\overline{W}}$ has degree $\ell - 2$. For any σ of order not divisible by p, its Jordan form is obtained from that of $\sigma_{|\overline{W}}$, adding a unique block I_2.

3. The case $n \in \{9, 11, 13, 17\}$

In this section, we take $J = \mathrm{diag}\left(\mathrm{I}_{n-3}, \left(\begin{smallmatrix} 0&0&1 \\ 0&1&0 \\ 1&0&0 \end{smallmatrix}\right)\right)$ of determinant -1. For any $a \in \mathbb{F}_q^*$, we define four matrices $x_1, x_2, y_1, y_2 \in \mathrm{SL}_n(q)$ with $x_i^2 = y_i^3 = \mathrm{I}_n$ as follows.

(x_1) x_1 acts on $\mathscr{C} = \{e_1, \ldots, e_n\}$ as:

- the identity if $n = 9$;
- the permutation $(e_1, e_3)(e_2, e_4)$ if $n = 11$;
- the permutation $(e_1, e_2)(e_4, e_5)$ if $n = 13$;
- the permutation $(e_1, e_3)(e_2, e_4)(e_5, e_6)(e_8, e_9)$ if $n = 17$.

(x_2) $x_2 = \mathrm{diag}(\mathrm{I}_{n-9}, \bar{x})$, where $\bar{x} = \bar{x}(a)$ is as in Figure 1.

(y_1) y_1 acts on $\mathscr{C}$ as:

- the identity if $n \in \{9, 11\}$;
- the permutation (e_2, e_3, e_4) if $n = 13$;
- the permutation $(e_3, e_4, e_5)(e_6, e_7, e_8)$ if $n = 17$.

(y_2) $y_2 = \mathrm{diag}(\mathrm{I}_{n-9}, \bar{y})$, where $\bar{y}$ is as in Figure 1.

We can see x_2 as the product of an even number of transpositions and the matrix $\mathrm{diag}(\mathrm{I}_{n-3}, x_3)$ with $x_3 = \left(\begin{smallmatrix} 0&0&2/a \\ 0&-1&0 \\ a/2&0&0 \end{smallmatrix}\right)$. Identifying $\mathrm{Sym}(n-3)$ with the group of permutation matrices fixing $\{e_j \mid 1 \leq j \leq n-3\}$ and acting as the identity on $\langle e_{n-2}, e_{n-1}, e_n \rangle$, the first factor of x_2 viewed in $\mathrm{Sym}(n-3) \times \mathrm{GL}_3(q)$ is in $\mathrm{Alt}(n-3) \leq \Omega_n(q)$. In particular, it is an involution and the same applies to x_3. Similarly, also x_1 is the product of an even number of transpositions, so is in $\mathrm{Alt}(n-3) \leq \Omega_n(q)$. Moreover, $x_3 \in \Omega_3(q)$ if and only if $-a \in (\mathbb{F}_q^*)^2$. Indeed, x_3 is the product of the reflections with centres $\langle ae_{n-2} - 2e_n \rangle$ and $\langle e_{n-1} \rangle$, whose spinor norms are, respectively, $-2a(\mathbb{F}_q^*)^2$ and $\frac{1}{2}(\mathbb{F}_q^*)^2$.

https://doi.org/10.1017/S1446788724000016 Published online by Cambridge University Press

Clearly, y_1 and y_2 have determinant 1. Moreover, $y_1 \in \mathrm{Alt}(n-9) \leq \Omega_n(q)$ and $y_2^{\mathsf{T}} J y_2 = J$. Since $x_1x_2 = x_2x_1$ and $y_1y_2 = y_2y_1$, we conclude that $x := x_1x_2$ and $y := y_1y_2$ have respective orders 2 and 3, and

$$H := \langle x, y\rangle \leq \Omega_n(q) \quad \text{when } -a \in (\mathbb{F}_q^*)^2.$$

We also assume that $a \in \mathbb{F}_q^*$ is such that $\mathbb{F}_p[a] = \mathbb{F}_q$.

By direct computation, we see that the characteristic polynomial of xy is

$$\chi_{xy}(t) = (t+a)(t+a^{-1})(t^{n-2}-1) = t^n + (a+a^{-1})t^{n-1} + t^{n-2} - t^2 - (a+a^{-1})t - 1.$$

In particular, $\mathrm{tr}(xy) = -(a+a^{-1})$. Moreover, the minimal polynomial of xy is

$$\min_{xy}(t) = \begin{cases} (t+1)(t^{n-2}-1) & \text{if } a = 1,\\ (t+a)(t+a^{-1})(t^{n-2}-1) & \text{otherwise.}\end{cases}$$

If $a \neq 1$, the minimal polynomial of xy coincides with its characteristic polynomial. Hence, consideration of the canonical rational form of xy when $a \neq 1$ and direct computation when $a = 1$ tell us that $(xy)^{n-2} \neq \mathrm{I}_n$ has a fixed point space of dimension $n-2$, namely it is a *bireflection*.

Lemma 3.1. *For $1 \leq j, k \leq n-3$, there exists $h \in H$ such that $he_j = e_k$.*

Proof. Clearly, it is enough to show that, for $k \leq n-3$, there exists $h \in H$ such that $he_1 = e_k$. Noting that $ye_1 = e_2$, $ye_2 = e_3$, $xe_3 = e_4$, $ye_4 = e_5$ for $n = 9$, $xe_1 = e_3$, $ye_3 = e_4$, $ye_4 = e_5$, $xe_4 = e_2$ for $n \in \{11, 17\}$, and $xe_1 = e_2$, $ye_2 = e_3$, $ye_3 = e_4$ $xe_4 = e_5$ for $n = 13$, our claim is true for $k \leq 5$.

Now, let $5 \leq \ell \leq n-3$ be the largest integer for which, for all $1 \leq i \leq \ell$, there exists $h_i \in H$ such that $h_ie_1 = e_i$. If $\ell < n-3$, there exists $h \in \{x, y\}$ such that $he_\ell = e_{\ell+1}$, which is a contradiction. □

Lemma 3.2. *Assume $a^2 - a - 1 \neq 0$ if $n = 9$, $(a-1)(a^3 + 2a^2 + a + 1) \neq 0$ if $n = 11$ and $a^4 + a^2 - a + 1 \neq 0$ if $n = 17$. Then, the group H is absolutely irreducible.*

Proof. Assume, for a contradiction, that U is a proper H-invariant subspace. Define

$$g_9 = [x, y], \quad g_{11} = (xy^2)^3xy, \quad g_{13} = (xy^2)^2xy, \quad g_{17} = (xy^2)^6xy.$$

Under our hypotheses on a, for $n = 9$, we have $V_1(g_9) = \langle e_1\rangle$. By Corollary 2.2, we may assume $e_1 \in U$ and hence $e_1, \ldots, e_{n-3} \in U$ by Lemma 3.1. Similarly, for $n = 11$, we have $V_1(g_{11}) = \langle e_3\rangle$, for $n = 13$, we have $V_1(g_{13}) = \langle e_2\rangle$ and for $n = 17$, we have $V_1(g_{17}) = \langle e_6\rangle$. In all these cases, as above, we may assume $e_1, \ldots, e_{n-3} \in U$. Noting that $ye_{n-3} + e_{n-3} = -2e_{n-2}$, $y^2e_{n-5} = e_{n-1}$ and $y^2e_{n-2} = -\frac{1}{2}e_n$, we get the contradiction $U = V$. □

For the following result, we need the traces of $[x, y]^j$, $j = 1, 2$:

$$\mathrm{tr}([x, y]) = 1 + a^2 + a^{-2} + \varsigma_n \quad \text{and} \quad \mathrm{tr}([x, y]^2) = (1 + a^2 + a^{-2})^2 - 4a - \kappa_n,$$

https://doi.org/10.1017/S1446788724000016 Published online by Cambridge University Press

where

$$\varsigma_n = \begin{cases} 1 & \text{if } n = 9, \\ 0 & \text{otherwise} \end{cases} \quad \text{and} \quad \kappa_n = \begin{cases} 3 & \text{if } n = 9, \\ 2 & \text{if } n = 11, \\ 4 & \text{if } n = 13, 17. \end{cases}$$

LEMMA 3.3. *The group H is not contained in any maximal subgroup M in class C_5 of $\Omega_n(q)$.*

PROOF. Suppose the contrary. By [1, Tables 8.58 and 8.74] and [5, Proposition 4.5.8], we have either $M \cong \Omega_n(q_0)$ where $q = q_0^r$ and r is an odd prime, or $M \cong \mathrm{SO}_n(q_0)$ where $q = q_0^2$. Thus, there exists $g \in \mathrm{GL}_n(\mathbb{F})$ such that $x^g = x_0$, $y^g = y_0$, with $x_0, y_0 \in \mathrm{GL}_n(q_0)$. From $\mathrm{tr}([x,y]^j) = \mathrm{tr}([x^g, y^g]^j) = \mathrm{tr}([x_0, y_0]^j)$, $j = 1, 2$, it follows that $4a + \kappa_n = (\mathrm{tr}([x,y]) - \varsigma_n)^2 - \mathrm{tr}([x,y]^2) \in \mathbb{F}_{q_0}$, whence $a \in \mathbb{F}_{q_0}$. So, $\mathbb{F}_q = \mathbb{F}_p[a] \leq \mathbb{F}_{q_0}$ implies $q_0 = q$. □

LEMMA 3.4. *Assume $a^2 - a - 1 \neq 0$ for $n = 9$. If H is absolutely irreducible, then H is not contained in any monomial subgroup of $\Omega_n(q)$.*

PROOF. For the sake of contradiction, suppose that H is contained in a monomial subgroup $M \in C_2$ of $\Omega_n(q)$. In this case, we may assume $q = p$ and H acts monomially with respect to an orthonormal basis $\mathcal{B} = \{v_1, v_2, \ldots, v_n\}$, see [5, Proposition 4.2.15]. Moreover, by [1, Tables 8.58 and 8.74] and [5, Proposition 4.5.8], the order of M divides $2^{n-1}|\mathrm{Sym}(n)|$. In particular, any prime divisor ϱ of $|H|$ should satisfy $\varrho \leq n$. If we can show that $e_1 \in \mathcal{B}$, we easily get a contradiction. Indeed, from $e_1 \in \mathcal{B}$, it follows that $e_i \in \mathcal{B}$ for all $1 \leq i \leq n-3$ (see Lemma 3.1). Hence, we may assume $v_i = e_i$ for $1 \leq i \leq n-3$. In particular, $e_{n-3} \in \mathcal{B}$. As $ye_{n-3} = -2e_{n-2} - e_{n-3}$ is not an element of $\langle e_i \mid 1 \leq i \leq n-3 \rangle$, ye_{n-3} should be orthogonal to v_{n-3} obtaining the contradiction $v_{n-3}^{\mathsf{T}} J y e_{n-3} = e_{n-3}^{\mathsf{T}} J y e_{n-3} = -1 \neq 0$.

So, we now show that $e_1 \in \mathcal{B}$. To this purpose, note that if $\mathrm{tr}(h) \neq 0$, then h must fix at least one $\langle v_j \rangle$. Moreover, given $h \in H$ of order k, $h\langle v_j \rangle = \langle v_j \rangle$ implies $hv_j = \lambda v_j$, with $\lambda = \pm 1$. So, consider the permutation ζ induced by h on the $\langle v_i \rangle$. If ζ^b acts as the identity on $\{\langle v_1 \rangle, \langle v_2 \rangle, \ldots, \langle v_n \rangle\}$ for some $b \geq 1$, then $h^b v_i = \pm v_i$ for every i. It follows that ζ has order k or $k/2$. In particular, if h has odd order, it permutes $\mathcal{B}$ and its cycle structure is determined by its rational canonical form. Also, if $h \in H$ does not have the eigenvalue -1, from $h\langle v_j \rangle = \langle v_j \rangle$, we get $hv_j = v_j$. Clearly, this applies to $h = y$. Since y has order 3, setting $r = 0$ if $n = 9$, $r = 1$ if $n = 13$ and $r = 2$ if $n \in \{11, 17\}$, y fixes v_j for $1 \leq j \leq r$ and permutes the remaining vectors v_j in $(n-r)/3$ orbits of length 3.

Case $n = 11, 13, 17$. Call s the number of vectors $u_j = e_j + ye_j + y^2 e_j$, with $ye_j \neq e_j$, fixed by y. Then, any $v_1 \in V_1(y)$ can be written as

$$v_1 = \sum_{i=1}^{r} \alpha_i e_i + \sum_{j=1}^{s} \beta_j u_j.$$

https://doi.org/10.1017/S1446788724000016 Published online by Cambridge University Press

Substituting e_i by $\lambda_i e_i$ and u_j by $\mu_j u_j$ if necessary, we may assume that all the coefficients α_i, β_j are in $\{0, 1\}$. Since y fixes v_1, by the transitivity of H on the subspaces generated by the vectors of $\mathcal{B}$, due to its irreducibility, we may also assume $v_3 = xv_1$, $v_4 = yv_3$, $v_5 = yv_4$ and $v_6 = xv_5$. Imposing $v_1^{\mathsf{T}} J v_3 = v_j^{\mathsf{T}} J v_6 = 0$ for all $j \in \{1, 4, 5\}$, we get $v_1 \in \{e_1, \ldots, e_r\}$, unless $n \in \{11, 17\}$, $q = 3$ and $a = -1$. In these exceptional cases, by direct computation, the order of $(xy)^2 xy^2$ is divisible by a prime $\varrho \geq 41$, which is a contradiction as ϱ does not divide $|\mathrm{Sym}(n)|$, $n \leq 17$ (see the beginning of the proof).

Case $n = 9$. Take $h = [x, y]$ and suppose $a^2 - a - 1 \neq 0$. Then $V_1([x, y]) = \langle e_1 \rangle$. We have

$$\mathrm{tr}(h) = \frac{(a^2+1)^2}{a^2} \quad \text{and} \quad \chi_h(-1) = \frac{-8(a^2+a+1)^2}{a^2}.$$

It follows $e_1 \in \mathcal{B}$ unless, possibly, when $a^2 + 1 = 0$ or $a^2 + a + 1 = 0$. As previously remarked, the order of any element of M, and hence *a fortiori* of H, if odd must belong to the set $\{1, 3, 5, 7, 9, 15\}$, and if prime must belong to $\{2, 3, 5, 7\}$. Assume $a^2 + 1 = 0$. If $p \neq 5$, we may take $h = [x, y]^2$, as $V_1(h) = \langle e_1 \rangle$ and $\mathrm{tr}(h) = -4a - 2 \neq 0$. If $q = 5$, then $a = 2$ and $[x, y]$ has order $156 = 2^2 \cdot 3 \cdot 13$, which is a contradiction. So, assume $a^2 + a + 1 = 0$. If $p \neq 3$, the permutation induced by xy on the $\langle v_i \rangle$ has order divisible by 21, which is a contradiction. If $q = 3$, then $a = 1$ and $[x, y]^3 y$ has order 41, which is a contradiction. □

LEMMA 3.5. *Assume $n = 9$. If the group H is absolutely irreducible, then it is neither contained in a maximal subgroup in class C_2 of $\Omega_9(q)$ nor contained in any maximal subgroup in class C_7.*

PROOF. For the sake of contradiction, suppose that H is imprimitive. By Lemma 3.4, we may assume $H \leq M \cong \Omega_3(q)^3.2^4.\mathrm{Sym}(3)$, where M permutes a decomposition $\mathbb{F}_q^9 = W_1 \oplus W_2 \oplus W_3$, with $\dim(W_i) = 3$. Set $h = (xy)^7$ and $N = \Omega_3(q)^3$. From $\dim(V_1(h)) = 7$, we get $V_1(h) \cap W_i \neq \{0\}$, whence $hW_i = W_i$ for each $i = 1, 2, 3$. It follows that $(xy)^7 \in N$. Since 7 is coprime to the index of N in M, we get $xy \in N$. Since y acts as a 3-cycle on $\{W_1, W_2, W_3\}$, it follows that the elements $(xy)^i y$, $1 \leq i \leq 7$, have trace equal to zero. Thus, $0 = \mathrm{tr}(xy^2) = -(a + a^{-1})$ gives the condition $a^2 + 1 = 0$. In this case, $\mathrm{tr}((xy)^3 y) = 1$, which is a contradiction.

Now, suppose that H is contained in a maximal subgroup M in class C_7 of $\Omega_n(q)$. By [1, Table 8.58], $M \cong \Omega_3(q)^2.[4]$. Then, $h = (xy)^7$ belongs to $\Omega_3(q)^2$. Suppose first that xy is semisimple. Up to conjugation, $h = \mathrm{diag}(\beta_1, 1, \beta_1^{-1}) \otimes \mathrm{diag}(\beta_2, 1, \beta_2^{-1})$ for some $\beta_1, \beta_2 \in \mathbb{F}_q^*$. In order that it has the eigenvalue 1 with multiplicity (at least) 7, we need $\beta_1 = \beta_2 = 1$, which gives $h = \mathrm{I}_9$, which is a contradiction. Finally, assume that xy has order divisible by p. Up to conjugation and because of (2.1),

$$h = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix} \otimes \begin{pmatrix} \beta & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \beta^{-1} \end{pmatrix}, \quad \beta \in \mathbb{F}_q^*.$$

https://doi.org/10.1017/S1446788724000016 Published online by Cambridge University Press

Hence, $\chi_h(t) = (t-1)^3(t-\beta)^3(t-\beta^{-1})^3$. Since h is a bireflection (that is, $\dim(V_1(h)) = 7$), we must have $\beta = 1$, in which case $\dim(V_1(h)) = 3$, which is a contradiction. □

LEMMA 3.6. *If H is absolutely irreducible, then the H-module $V = \mathbb{F}^n$ is not the deleted permutation module of degree $\ell = n+1, n+2$.*

PROOF. Assume the contrary. From what is seen at the end of Section 2, up to conjugation, we may assume $H \le \mathrm{Sym}(\ell) \le \mathrm{GL}_\ell(p)$, with $\ell = n+1, n+2$.

Case $\ell = n+1$. Fix $h \in H$ such that $\dim(V_1(h)) = 1$ and call ζ its preimage in $\mathrm{Sym}(\ell) \le \mathrm{GL}_\ell(p)$. Then, ζ has at most two orbits. It follows that $\mathrm{tr}(\zeta) = 0$ if ζ is an ℓ-cycle or the product of two cycles of length at least two. Otherwise, $\mathrm{tr}(\zeta) = 1$ and ζ is a cycle of length $\ell - 1$. Note that ζ and h have the same order.

We may take $h = xy$, as $\dim(V_1(xy)) = 1$. Hence, $\mathrm{tr}(\zeta) - 1 = \mathrm{tr}(xy) = -(a + a^{-1})$ gives the following two cases: if $\mathrm{tr}(\zeta) = 0$, then $a^2 - a + 1 = 0$; if $\mathrm{tr}(\zeta) = 1$, then $a^2 + 1 = 0$. In the second case, the characteristic polynomial $\chi_{xy}(t)$ is divisible by $t^2 + 1$, and then xy has order divisible by 4. However, ζ has odd order n, being an n-cycle, which is a contradiction.

So, assume $a^2 - a + 1 = 0$. In this case, $t^2 + t + 1$ divides $\chi_{xy}(t)$ and hence the order of ζ is divisible by 3. Furthermore, $(xy)^{n-2}$ has order p when $n \in \{11, 17\}$. For $n = 11$, we get that the order of ζ is 6, 9 or 12, in contrast with $(xy)^9$ of odd order p. For $n = 17$, the order of ζ is 9, 12, 15 or 18. However, $(xy)^9 \ne \mathrm{I}_{17}$ and the other values are in contrast with $(xy)^{15}$ of odd order p. For $n \in \{9, 13\}$, we apply the previous argument to other elements h such that $\dim(V_1(h)) = 1$. For $n = 9$, we take $h = [x, y]$ whose trace is equal to 1, which is a contradiction. For $n = 13$, we take $h = (xy^2)^2 xy$, which has trace equal to 3. Since $\mathrm{tr}(h) = \mathrm{tr}(\zeta) - 1 \in \{-1, 0\}$, we get an absurdity unless $p = 3$. However, in this case, $a = -1$ and h^8 has order 41, which is a contradiction as $h^8 \in H \le \mathrm{Sym}(14)$.

Case $\ell = n+2$. In this case, $q \mid \ell$, and hence we need to consider only the following cases: (a) $(n, q) = (9, 11)$; (b) $(n, q) = (11, 13)$; (c) $(n, q) = (13, 3)$; (d) $(n, q) = (13, 5)$; (e) $(n, q) = (17, 19)$. Take $g = (xy)^3(xy^2)^7$ in case (a); $g = xy(xy^2)^2$ in cases (b), (c) and (e); and $g = xy(xy^2)^3$ in case (d). By direct computation, in all these cases, the order of g is divisible by a prime $\varrho \ge n + 4$, which is a contradiction as ϱ should divide $|\mathrm{Sym}(n+2)|$. □

THEOREM 3.7. *Suppose $n \in \{9, 11, 13, 17\}$ and let $a \in \mathbb{F}_q^*$ be such that:*

(i) $\mathbb{F}_p[a] = \mathbb{F}_q$;
(ii) $-a \in (\mathbb{F}_q^*)^2$;
(iii) $$\begin{cases} a^2 - a - 1 \ne 0 & \text{if } n = 9; \\ (a-1)(a^3 + 2a^2 + a + 1) \ne 0 & \text{if } n = 11; \\ a^4 + a^2 - a + 1 \ne 0 & \text{if } n = 17. \end{cases}$$

Then, $H = \Omega_n(q)$. In particular, $\Omega_n(q)$ is $(2, 3)$-generated for any odd q.

PROOF. By condition (ii), H is a subgroup of $\Omega_n(q)$. By condition (iii), Lemmas 3.2, 3.4 and 3.5, the group H is absolutely irreducible and is neither contained in a maximal subgroup in class C_2 of $\Omega_n(q)$ nor contained in any maximal subgroup in class C_7. Since it contains the bireflection $(xy)^{n-2}$, we can apply [3, Theorem 7.1] which, combined with condition (i) and Lemma 3.3, gives two possibilities: (a) H is an alternating or symmetric group of degree ℓ and $\mathbb{F}^n$ is the deleted permutation module of dimension $\ell - 1$ or $\ell - 2$; (b) $H = \Omega_n(q)$. Case (a) is excluded by Lemma 3.6: we conclude that $H = \Omega_n(q)$.

Finally, we have to prove that there exists an element a satisfying all the requirements. If $q = p$, take $a = -1$. Suppose now $q = p^f$ with $f \geq 2$, and let $\mathcal{N}(q)$ be the number of elements $b \in \mathbb{F}_q^*$ such that $\mathbb{F}_p[b] \neq \mathbb{F}_q$. By [12], we have $\mathcal{N}(q) \leq p(p^{\lfloor f/2 \rfloor} - 1)/(p-1)$, and hence it suffices to check when $(p^f - 1)/2 - p(p^{\lfloor f/2 \rfloor} - 1)/(p-1) > 4$. This condition is fulfilled unless $q = 3^2$. So, assume $q = 9$ and take $a \in \mathbb{F}_9^*$ whose minimal polynomial over $\mathbb{F}_3$ is $t^2 + 1$. Then, $\mathbb{F}_3[a] = \mathbb{F}_9$ and $-a = (a+1)^2$ is a square. □

4. Generators for $n \in \{12, 15, 16\}$ and for $n \geq 18$

For $n \in \{12, 15, 16\}$ and for $n \geq 18$, write $n = 3m + 9 + r$, with $m \geq 1$ and $r \in \{0, 1, 2\}$. Take the symmetric bilinear form corresponding to the Gram matrix $J = \begin{pmatrix} \mathrm{I}_{n-8} & 0 & 0 \\ 0 & 0 & \mathrm{I}_4 \\ 0 & \mathrm{I}_4 & 0 \end{pmatrix}$, having $\det(J) = 1$. For any $a \in \mathbb{F}_q^*$, we define four matrices x_1, x_2, y_1, y_2 of $\mathrm{GL}_n(q)$ as follows.

(x_1) x_1 acts on $\mathscr{C}$ as the product $\nu_1\nu_2$ of the following two disjoint permutations:

$$\nu_1 = \begin{cases} \mathrm{id} & \text{if } r = 0 \text{ and } n \text{ is odd,} \\ (e_1, e_2) & \text{if } r = 0 \text{ and } n \text{ is even,} \\ (e_1, e_2) & \text{if } r = 1 \text{ and } n \text{ is odd,} \\ (e_1, e_2)(e_3, e_6) & \text{if } r = 1 \text{ and } n \text{ is even,} \\ (e_1, e_3)(e_2, e_4) & \text{if } r = 2 \text{ and } n \text{ is odd,} \\ (e_1, e_3)(e_2, e_4)(e_7, e_{10}) & \text{if } r = 2 \text{ and } n \text{ is even,} \end{cases}$$

and

$$\nu_2 = \prod_{j=0}^{m-1} (e_{3j+r+3}, e_{3j+r+4}) = (e_{r+3}, e_{r+4})(e_{r+6}, e_{r+7}) \cdots (e_{n-9}, e_{n-8}).$$

(x_2) $x_2 = \mathrm{diag}(\mathrm{I}_{n-9}, \tilde{x})$, where $\tilde{x} = \tilde{x}(a)$ is as in Figure 2.

(y_1) y_1 acts on $\mathscr{C}$ as the permutation

$$\nu_3 = \prod_{j=0}^{m-1} (e_{3j+r+1}, e_{3j+r+2}, e_{3j+r+3})$$
$$= (e_{r+1}, e_{r+2}, e_{r+3})(e_{r+4}, e_{r+5}, e_{r+6}) \cdots (e_{n-11}, e_{n-10}, e_{n-9}).$$

(y_2) $y_2 = \mathrm{diag}(\mathrm{I}_{n-9}, \tilde{y})$, where $\tilde{y}$ is as in Figure 2.

$$\tilde{x} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & a & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & a \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}, \quad \tilde{y} = \begin{pmatrix} -1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -\frac{1}{2} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ -2 & -2 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

FIGURE 2. Alternative generators of $\Omega_9(q)$.

Let us identify $\mathrm{Sym}(n-8)$ with the group of permutation matrices fixing the set $\{e_j \mid 1 \leq j \leq n-8\}$ and acting as the identity on $\langle e_{n-7}, e_{n-6}, \ldots, e_n\rangle$. The matrix x_1 is the product of N transpositions in $\mathrm{Sym}(n-8)$, where N is as follows:

	$r = 0$	$r = 1$	$r = 2$
n even	$N = m + 1$	$N = m + 2$	$N = m + 3$
n odd	$N = m$	$N = m + 1$	$N = m + 2$

Now, n is odd if and only if m and r have the same parity. It follows that N is always even, whence $x_1 \in \mathrm{Alt}(n-8) \leq \Omega_n^\epsilon(q)$. In particular, x_1 is an involution and the same is easily verified for x_2. To see that $x_2 \in \Omega_n^\epsilon(q)$, note that $\tilde{x} = \mathrm{diag}(1, h, h^{-\mathsf{T}})$ with $h \in \mathrm{SL}_4(q)$. Since $\mathrm{diag}(1, g, g^{-\mathsf{T}}) \in \mathrm{SO}_9(q)$ for each $g \in \mathrm{GL}_4(q)$, we conclude that $\tilde{x}$ is in $\Omega_9(q)$.

Clearly, y_1 and y_2 have order 3 and determinant 1. Moreover, $y_1 \in \mathrm{Alt}(n-9) \leq \Omega_n^\epsilon(q)$ and $y_2^{\mathsf{T}} J y_2 = J$. Since $x_1x_2 = x_2x_1$ and $y_1y_2 = y_2y_1$, we conclude that $x = x_1x_2$ and $y = y_1y_2$ have respective orders 2 and 3, and that

$$H := \langle x, y\rangle \leq \Omega_n^\epsilon(q).$$

We also assume that $a \in \mathbb{F}_q^*$ is such that $\mathbb{F}_p[a] = \mathbb{F}_q$.

When $n \neq 12$, we can decompose $\mathbb{F}_q^n$ into the direct sum of the following $[x, y]$-invariant subspaces. Take

$$\mathcal{A} = \begin{cases} \langle e_1, e_3, e_4\rangle & \text{if } n = 15, \\ \langle e_1, e_5\rangle \oplus \langle e_2, e_4\rangle & \text{if } n = 16, \\ \langle e_1, e_2, e_4, e_5\rangle \oplus \langle e_3, e_7, e_8\rangle & \text{if } n = 19, \\ \langle e_1, e_2, e_6, e_8\rangle \oplus \langle e_3, e_4, e_5, e_9\rangle & \text{if } n = 20, \\ \langle e_1, e_2, e_3, e_4, e_5, e_6, e_8, e_9\rangle \oplus \langle e_7, e_{11}, e_{12}\rangle & \text{if } n = 23. \end{cases}$$

https://doi.org/10.1017/S1446788724000016 Published online by Cambridge University Press

Otherwise,

$$\mathcal{A} = \begin{cases} \langle e_1, e_2, e_3, e_4, e_6, e_7 \rangle & \text{if } r = 0, \\ \langle e_1, e_2, e_4, e_5 \rangle \oplus \langle e_3, e_6, e_7, e_8, e_{10}, e_{11} \rangle & \text{if } r = 1, \\ \langle e_1, e_2, e_3, e_4, e_5, e_6, e_8, e_9 \rangle \oplus \langle e_7, e_{10}, e_{11}, e_{12}, e_{14}, e_{15} \rangle & \text{if } r = 2. \end{cases}$$

Moreover,

$$\mathcal{B} = \bigoplus_{j=0}^{m-4-r} \langle e_{5+4r+3j}, e_{9+4r+3j}, e_{10+4r+3j} \rangle,$$
$$C = \langle e_{n-13}, e_{n-10}, e_{n-9}, e_{n-8}, e_{n-7}, e_{n-6}, e_{n-5}, e_{n-4}, e_{n-3}, e_{n-2}, e_{n-1}, e_n \rangle.$$

LEMMA 4.1. *Assume $n \neq 12$. Then, $([x, y]_{|\mathcal{A}})^{24} = \mathrm{I}$ and $([x, y]_{|\mathcal{B}})^3 = \mathrm{I}$.*

PROOF. For $n \in \{15, 16, 19, 20, 23\}$, the element $[x, y]$ acts on $\mathcal{A}$ as the following permutation:

$$\begin{cases} (e_3, e_4) & \text{if } n = 15, \\ (e_1, e_5)(e_2, e_4) & \text{if } n = 16, \\ (e_1, e_5, e_4, e_2)(e_3, e_8, e_7) & \text{if } n = 19, \\ (e_1, e_6, e_8, e_2)(e_3, e_4, e_9, e_5) & \text{if } n = 20, \\ (e_1, e_6, e_5, e_3, e_4, e_9, e_8, e_2)(e_7, e_{12}, e_{11}) & \text{if } n = 23. \end{cases}$$

Otherwise, it acts on $\mathcal{A}$ as

$$\begin{cases} (e_1, e_4, e_3, e_2, e_7, e_6) & \text{if } n \equiv 0 \pmod 6, \\ (e_1, e_5, e_4, e_2)(e_3, e_8, e_7)(e_6, e_{11}, e_{10}) & \text{if } n \equiv 1 \pmod 6, \\ (e_1, e_6, e_8, e_2)(e_3, e_4, e_9, e_5)(e_7, e_{12}, e_{11}, e_{10}, e_{15}, e_{14}) & \text{if } n \equiv 2 \pmod 6, \\ (e_2, e_7, e_6)(e_3, e_4) & \text{if } n \equiv 3 \pmod 6, \\ (e_1, e_5)(e_2, e_4)(e_3, e_8, e_7, e_6, e_{11}, e_{10}) & \text{if } n \equiv 4 \pmod 6, \\ (e_1, e_6, e_5, e_3, e_4, e_9, e_8, e_2)(e_7, e_{12}, e_{11})(e_{10}, e_{15}, e_{14}) & \text{if } n \equiv 5 \pmod 6. \end{cases}$$

Finally, $[x, y]$ acts on each summand of $\mathcal{B}$ as the cycle $(e_{5+4r+3j}, e_{10+4r+3j}, e_{9+4r+3j})$. □

By Lemma 4.1 and direct computations (in particular, for $n = 12$), the element $\tau = [x, y]^{24}$ has characteristic polynomial $(t - 1)^n$. More precisely, setting

https://doi.org/10.1017/S1446788724000016 Published online by Cambridge University Press

$$\vartheta_0 = \begin{pmatrix} 1 & 0 & -4a & 0 & -32a^2 & -36a^2 & -8a & -56a^2 \\ 0 & 1 & -4a & 0 & -28a^2 & -32a^2 & -8a & -64a^2 \\ 0 & 0 & 1 & 0 & 8a & 8a & 0 & 16a \\ 0 & 0 & -8a & 1 & -72a^2 & -64a^2 & -16a & -128a^2 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 4a & 4a & 1 & 8a \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

we have $\tau = \mathrm{diag}(\mathrm{I}_{n-8}, \vartheta)$, where

$$\vartheta = \vartheta_0 + 8(E_{1,6} + 2E_{2,8} + 2E_{4,5} - E_{2,5} - 2E_{1,8} - 2E_{4,6})$$

if $n \in \{12, 16, 20\}$, and $\vartheta = \vartheta_0$ otherwise. Notice that the minimal polynomial of ϑ is $(t-1)^3$. It follows that τ is an element of order p fixing the 9-dimensional subspace $S_9 = \langle e_{n-8}, e_{n-7}, \ldots, e_n\rangle$. Furthermore, the fixed point space of $\tau_{|S_9}$ has dimension 5, unless $n \in \{12, 16, 20\}$ and $a^2 = 3$, in which case it has dimension 7.

5. The case $n \in \{15, 18, 19\}$ or $n \geq 21$

The subspace S_9 is invariant under $K = \langle y, \tau\rangle$: our first aim is to find conditions on $a \in \mathbb{F}_q^*$ so that $K_{|S_9} = \Omega_9(q)$. In the following, we identify y, τ with their restrictions to S_9.

LEMMA 5.1. *The group $K_{|S_9}$ is absolutely irreducible.*

PROOF. We apply Corollary 2.2 to $g = [y, \tau]$ and $\lambda = 1$. So, we may assume that the eigenvector $s = e_{n-8} - e_{n-7}$ is contained in U. Take the matrices M_1, M_2, whose columns are the images of s under the following elements:

$$\begin{aligned} M_1 :&\quad \mathrm{I}_9,\ y,\ y^2,\ \tau y^2,\ \tau^2 y^2,\ y\tau y^2,\ y^2\tau y^2,\ y\tau^2 y^2,\ y^2\tau^2 y^2; \\ M_2 :&\quad \mathrm{I}_9,\ y,\ y^2,\ \tau y^2,\ \tau^2 y^2,\ y\tau y^2,\ y\tau^2 y^2,\ (\tau y^2)^2,\ \tau y^2\tau^2 y^2. \end{aligned}$$

Then, $\det(M_1) = -2^{35}a^{10}(4a^2 + 3)$ and $\det(M_2) = -2^{35}a^{10}(28a^2 - 3)$. Clearly, these two matrices cannot be both singular, whence $\dim(U) = 9$, which is a contradiction. □

LEMMA 5.2. *The group $K_{|S_9}$ is neither monomial nor contained in any maximal subgroup* $\mathrm{PSL}_2(8)$, $\mathrm{PSL}_2(17)$, $\mathrm{Alt}(10)$, $\mathrm{Sym}(10)$, $\mathrm{Sym}(11)$ *in class $\mathcal{S}$ of* $\Omega_9(q)$.

PROOF. Recall that τ is an element of order p. Considering the order of the maximal subgroups M described in the statement and the conditions on q given in [1, Tables 8.58 and 8.59], we may reduce to the following cases:

(i) $M = 2^8 : \mathrm{Alt}(9)$ and $q \in \{3, 5\}$;
(ii) $M = 2^8 : \mathrm{Sym}(9)$ and $q = 7$;
(iii) $M = \mathrm{Alt}(10)$ and $q \in \{3, 7\}$;
(iv) $M = \mathrm{PSL}_2(17)$ and $q = 9$;
(v) $M = \mathrm{Sym}(11)$ and $q = 11$;
(vi) $M = \mathrm{PSL}_2(8)$ and $q = 27$.

https://doi.org/10.1017/S1446788724000016 Published online by Cambridge University Press

Now, we look for an element of H whose order does not divide $|M|$. In particular, it suffices to find an element of H whose order is divisible by a prime $\varrho > 17$ in case (iv), $\varrho > 11$ otherwise. Define $g_j = y\tau^j$. If $q \in \{3, 9\}$, then g_1 has order divisible by 41. If $q = 5$, then g_3 has order divisible by a prime $\varrho \geq 13$. If $q = 7$, take $j = 2$ when $a = \pm 2$, and $j = 3$ when $a \in \{\pm 1, \pm 3\}$. Then, the order of g_j is divisible by a prime $\varrho \geq 43$. If $q = 11$, take $j = 2$ if $a = \pm 5$ and $j = 1$ otherwise. Then the order of g_j is divisible by a prime $\varrho \geq 19$. Finally, if $q = 27$, then g_2 has order divisible by 37. In all these cases, we easily obtain a contradiction. □

For the next lemma, we use the following traces of elements of $K_{|S_9}$:

$$\mathrm{tr}((y\tau)^2) = -2176a^4 + 128a^2, \quad \mathrm{tr}((y^2\tau)^2) = 1920a^4 + 128a^2. \tag{5-1}$$

LEMMA 5.3. *The group $K_{|S_9}$ is neither contained in a maximal subgroup in class C_2 of $\Omega_9(q)$ nor contained in any maximal subgroup in class C_7.*

PROOF. By Lemma 5.2, the group $K_{|S_9}$ is not monomial. So, suppose that $K_{|S_9}$ preserves a nonsingular decomposition $\mathbb{F}_q^9 = W_1 \oplus W_2 \oplus W_3$ with $\dim(W_i) = 3$. Clearly, for each $k \in K_{|S_9}$, its cube fixes each W_i, preserving a nonsingular symmetric form. Thus, its eigenvalues are $\pm 1, \alpha_i, \alpha_i^{-1}$. It follows that k^3 must have the eigenvalue 1 with multiplicity at least 3, or the eigenvalue -1 with multiplicity at least 2. Assume first $p = 3$. We have $\chi_{(y\tau)^3}(t) = (t-1)f(t)$, where $f(t) = t^8 + t^7 - (a^{12} + a^6 - 1)t^6 - (a^{12} - 1)t^5 - (a^6 - 1)t^4 - (a^{12} - 1)t^3 - (a^{12} + a^6 - 1)t^2 + t + 1$. Then, $f(1) = -a^{12} \neq 0$ and $f(-1) = 1$, which is a contradiction. Next, assume $p \neq 3$. From $\mathrm{tr}(\tau) = 9 \neq 0$, we get that τ fixes each W_i. By the irreducibility of $K_{|S_9}$, the element y acts on $\{W_1, W_2, W_3\}$ as the 3-cycle (W_1, W_2, W_3). In this case, both $(y\tau)^2$ and $(y^2\tau)^2$ should have trace 0, in contrast with (5.1) which gives $0 = \mathrm{tr}((y^2\tau)^2) - \mathrm{tr}((y\tau)^2) = 2^{12}a^4$.

Finally, suppose that $K_{|S_9}$ is contained in a maximal subgroup $M \cong \Omega_3(q)^2.[4] \in C_7$, and hence actually in $\Omega_3(q)^2$. Up to conjugation, we may suppose $\tau = \begin{pmatrix} 1&1&1\\0&1&2\\0&0&1 \end{pmatrix} \otimes \begin{pmatrix} 1&1&1\\0&1&2\\0&0&1 \end{pmatrix}$. The dimensions of the fixed point space of this tensor product and of τ are, respectively, 3 and 5, which is a contradiction. □

LEMMA 5.4. *The group $K_{|S_9}$ is not contained in any maximal subgroup $M \cong \mathrm{PSL}_2(q).2$ or $M \cong \mathrm{PSL}_2(q^2).2$ in class $\mathcal{S}$ of $\Omega_9(q)$.*

PROOF. Suppose the contrary.

Case $M \cong \mathrm{PSL}_2(q).2$. In this case, M arises from the representation $\Phi : \mathrm{GL}_2(q) \to \mathrm{GL}_9(q)$ obtained from the action of $\mathrm{GL}_2(q)$ on the space T of homogeneous polynomials of degree 8 in two variables t_1, t_2 over $\mathbb{F}_q$. Up to conjugation in $\mathrm{GL}_2(q)$, we may assume

$$\tau = \Phi(\mathrm{I}_2 + E_{1,2}) = \begin{cases} t_1 \mapsto t_1, \\ t_2 \mapsto t_1 + t_2. \end{cases}$$

https://doi.org/10.1017/S1446788724000016 Published online by Cambridge University Press

Direct computation (with respect to the basis $t_1^8, t_1^7t_2, \ldots, t_2^8$ of T) gives that the fixed point space of this linear transformation is generated by t_1^8. So, it has dimension 1, which is a contradiction as τ has a fixed point space of dimension 5.

Case $M \cong \mathrm{PSL}_2(q^2).2$. To understand M, start from the representation $\psi : \mathrm{GL}_2(q^2) \to \mathrm{GL}_3(q^2)$ described in (2.1). Next, consider the subspace W of $\mathrm{Mat}_3(q^2)$ consisting of the matrices A such that $A^{\mathsf{T}} = (a_{i,j}^q) = A^\sigma$. Clearly, W has dimension 9 over $\mathbb{F}_q$ and we may consider the representation $\Phi : \mathrm{GL}_3(q^2) \to \mathrm{GL}_9(q)$ induced by $A \mapsto (\psi(g))^{\mathsf{T}} A(\psi(g))^\sigma$ for all $g \in \mathrm{GL}_3(q^2)$. The group M arises from this representation. Again, up to conjugation in $\mathrm{GL}_2(q^2)$, we may suppose $\tau = \Phi(\psi(\mathrm{I}_2 + E_{1,2})) = \Phi\left(\begin{pmatrix} 1&1&1\\ 0&1&2\\ 0&0&1\end{pmatrix}\right)$. Direct calculation gives that the fixed point space of $\Phi(\psi(\mathrm{I}_2 + E_{1,2}))$ on $W \le \mathrm{Mat}_3(q^2)$ is generated by $E_{2,2}, E_{3,3}, E_{2,3} + E_{3,2}$. Thus, it has dimension 3, which is again a contradiction as τ has a fixed point space of dimension 5. □

PROPOSITION 5.5. *Suppose that q is odd and $n \in \{15, 18, 19\}$ or $n \ge 21$. Let $a \in \mathbb{F}_q^*$ be such that $\mathbb{F}_p[a] = \mathbb{F}_q$. Then, $K_{|S_9} = \Omega_9(q)$.*

PROOF. By Lemmas 5.1 and 5.3, $K_{|S_9}$ is absolutely irreducible, and is neither contained in a maximal subgroup in class C_2 of $\Omega_9(q)$ nor contained in any maximal subgroup in class C_7. Furthermore, by Lemmas 5.2 and 5.4, either $K_{|S_9} = \Omega_9(q)$ or $K_{|S_9}$ is contained in a maximal subgroup $M \in \{\Omega_9(q_0), \mathrm{SO}_9(q_0)\}$ in class C_5, where $q = q_0^r$ for some prime $r \ge 2$. Suppose there exists $g \in \mathrm{GL}_9(\mathbb{F})$ such that $\tau^g = \tau_0$, $y^g = y_0$, with $\tau_0, y_0 \in \mathrm{GL}_9(q_0)$. From $-2176a^4 + 128a^2 = \mathrm{tr}((y\tau)^2) = \mathrm{tr}((y^g\tau^g)^2) = \mathrm{tr}((y_0\tau_0)^2)$, it follows that $17a^4 - a^2 \in \mathbb{F}_{q_0}$. Similarly, from $\mathrm{tr}((y^2\tau)^2) = 1920a^4 + 128a^2$, we obtain $15a^4 + a^2 \in \mathbb{F}_{q_0}$. It follows that $32a^4 \in \mathbb{F}_{q_0}$ and then $a^2 \in \mathbb{F}_{q_0}$. Again, from $\mathrm{tr}(y^2\tau^2(y\tau)^2) = -49\,152a^6 + 16\,384a^5 + 3840a^4 + 256a^2 \in \mathbb{F}_{q_0}$, we get $a \in \mathbb{F}_{q_0}$. So, $\mathbb{F}_q = \mathbb{F}_p[a] \le \mathbb{F}_{q_0}$ implies $q_0 = q$, which is a contradiction. We conclude that $K_{|S_9} = \Omega_9(q)$. □

Define $E_0 = S_0 = \{0\}$ and, for $1 \le \ell \le n$,

$$E_\ell = \langle e_i \mid 1 \le i \le \ell\rangle \quad \text{and} \quad S_\ell = \langle e_i \mid n - \ell + 1 \le i \le n\rangle.$$

COROLLARY 5.6. *Suppose q odd and $n \in \{15, 18, 19\}$ or $n \ge 21$. Let $a \in \mathbb{F}_q^*$ be such that $\mathbb{F}_p[a] = \mathbb{F}_q$. Then:*

(i) $H = \Omega_n(q)$ *if n is odd;*
(ii) $H = \Omega_n^+(q)$ *if* $q \equiv 1 \pmod 4$ *and n is even;*
(iii) $H = \Omega_n^+(q)$ *if* $q \equiv 3 \pmod 4$ *and* $n \equiv 0 \pmod 4$*;*
(iv) $H = \Omega_n^-(q)$ *if* $q \equiv 3 \pmod 4$ *and* $n \equiv 2 \pmod 4$.

PROOF. By [1, Proposition 1.5.42(ii)], when n is even, we have $H \le \Omega_n^+(q)$ or $H \le \Omega_n^-(q)$ according as $n(q-1)/4$ is even or odd, respectively. Let ℓ be maximal with respect to

$$K_\ell := \mathrm{diag}(\mathrm{I}_{n-\ell}, \Omega_\ell^\epsilon(q)) \le H,$$

https://doi.org/10.1017/S1446788724000016 Published online by Cambridge University Press

where $\epsilon \in \{\circ, \pm\}$. Noting that $K' = \mathrm{diag}(\mathrm{I}_{n-9}, \Omega_9(q))$ by the previous proposition, we have that ℓ is at least 9 and we need to show that $\ell = n$. For the sake of contradiction, assume $9 \leq \ell < n$.

Suppose first that $(r, \ell) \notin \{(2, n-2), (2, n-1)\}$ and $(r, \ell) \notin \{(1, n-4), (2, n-8)\}$ when n is even. Then:

(a) if $\ell \equiv 0 \pmod 3$, then x fixes the subspaces $S_{\ell-1}$ and $E_{n-\ell-1}$, and acts as the transposition $(e_{n-\ell}, e_{n-\ell+1})$ on $\langle e_{n-\ell}, e_{n-\ell+1}\rangle$;

(b) if $\ell \equiv j \pmod 3$, with $j = 1, 2$, then y fixes the subspaces $S_{\ell-j}$ and $E_{n-\ell-3+j}$, and acts as $(e_{n-\ell-2+j}, e_{n-\ell-1+j}, e_{n-\ell+j})$ on $\langle e_{n-\ell-2+j}, e_{n-\ell-1+j}, e_{n-\ell+j}\rangle$.

Setting $g = x$ in case (a), and $g = y$ in case (b), we claim that $K_{\ell+1} := \langle K_\ell, K_\ell^g\rangle$ equals

$$\mathrm{diag}(\mathrm{I}_{n-\ell-1}, \Omega_{\ell+1}^{\overline{\epsilon}}(q)), \quad \overline{\epsilon} \in \{\circ, \pm\}. \tag{5-2}$$

Noting that $g^{-1}S_\ell$ is obtained from S_ℓ by replacing $e_{n-\ell+1}$ by $e_{n-\ell}$, one gets $\langle S_\ell, g^{-1}S_\ell\rangle = S_{\ell+1}$. Thus, $K_{\ell+1}$ fixes $S_{\ell+1}$, induces the identity on $E_{n-\ell-1}$ and fixes the restriction of J to $S_{\ell+1}$, of determinant 1. If follows that $K_{\ell+1}$ is contained in the group (5-2). Call ρ the matrix in $\mathrm{GL}_n(q)$ which acts according to $e_{n-\ell} \mapsto -e_{n-\ell}$, $e_{n-4} \mapsto -2e_n$, $e_n \mapsto -\frac{1}{2}e_{n-4}$ and fixes the remaining vectors e_i. Since ρ has determinant 1 and spinor norm $(\mathbb{F}_q^*)^2$, it belongs to K_ℓ^g, which induces Ω_ℓ^ϵ on $g^{-1}S_\ell$. Now, $\langle \rho, K_\ell\rangle$ is the stabilizer in the group (5-2) of the nondegenerate subspace $\langle e_{n-\ell}\rangle$. So, it is a maximal subgroup of the group (5-2). From $K_{\ell+1} \not\leq \langle \rho, K_\ell\rangle$, we get the final contradiction $K_{\ell+1} = \mathrm{diag}(\mathrm{I}_{n-\ell-1}, \Omega_{\ell+1}^{\overline{\epsilon}}(q))$.

It remains to exclude the exceptional cases: in each of them, we get the same contradiction.

Case 1. $r = 1$, $\ell = n-4$, n even. Let R be the stabilizer of e_6 in K_{n-4}. Then, $\langle R^x, K_{n-4}\rangle = K_{n-3}$, as it fixes the vectors e_1, e_2, e_3 and the subspace $E_3^\perp$, inducing $\Omega_{n-3}(q)$.

Case 2. $r = 2$, $\ell = n-8$, n even. Let R be the stabilizer of e_{10} in K_{n-8}. Then, $\langle R^x, K_{n-8}\rangle = K_{n-7}$, as it fixes the vectors $e_1, e_2, \ldots, e_7$ and the subspace $E_7^\perp$, inducing $\Omega_{n-7}(q)$.

Case 3. $r = 2$, $\ell = n-2$. Let R be the stabilizer of e_3 in K_{n-2}. Then, $\langle R^x, K_{n-2}\rangle = K_{n-1}$, as it fixes e_1 and $E_1^\perp$, inducing $\Omega_{n-1}^{\overline{\epsilon}}(q)$.

Case 4. $r = 2$, $\ell = n-1$. Similar to the above cases. □

6. The case $n \in \{12, 16, 20\}$

The values $n = 12, 16, 20$ require some small adjustments with respect to the general case, described in Section 5. So, in the proof of the following results, we only give the necessary modifications.

LEMMA 6.1. *Assume $a^2 \neq 2, 3$. Then, the group $K_{|S_9}$ is absolutely irreducible.*

PROOF. We have $s = e_{n-8} - e_{n-7}$ by the hypothesis $a^2 \neq 3$. Now, $\det(M_1) = -2^{35}a^6(a^2-2)(4a^4 - 13a^2 + 16)$ and $\det(M_2) = -2^{35}a^6(a^2-2)(28a^4 - 83a^2 - 16)$.

https://doi.org/10.1017/S1446788724000016 Published online by Cambridge University Press

Since $a^2 \neq 2$, the matrices M_1, M_2 are both singular only if $p = 13$ and $a^2 = 3$, which is excluded by hypothesis. □

LEMMA 6.2. *The group $K_{|S_9}$ is neither monomial nor contained in any maximal subgroup* $\mathrm{PSL}_2(8)$, $\mathrm{PSL}_2(17)$, $\mathrm{Alt}(10)$, $\mathrm{Sym}(10)$, $\mathrm{Sym}(11)$ *in class $\mathcal{S}$ of $\Omega_9(q)$.*

PROOF. If $q \in \{3, 5, 11\}$ proceed as in the proof of Lemma 5.2. If $q = 7$, take $j = 1$ if $a = \pm 1$ and $j = 3$ if $a = \pm 2$; take $\tilde{g} = \tau^2 y\tau y$ if $a = \pm 3$. Then, the order of g_j and the order of $\tilde{g}$ are divisible by a prime $\varrho \geq 43$. If $q = 9$, then g_1 has order divisible by 13, a prime that does divide $|\mathrm{PSL}_2(17)|$; if $q = 27$, then g_2 has order divisible by a prime $\varrho \in \{13, 73\}$. □

LEMMA 6.3. *Assume $a^2 \neq 3$. The group $K_{|S_9}$ is neither contained in a maximal subgroup in class C_2 of $\Omega_9(q)$ nor contained in any maximal subgroup in class C_7.*

PROOF. We proceed as in the proof of Lemma 5.3, describing only the necessary modifications to prove the primitivity of $K_{|S_9}$. For $p = 3$, we have $\chi_{(y\tau)^3}(t) = (t-1)f(t)$, where $f(t) = t^8 - t^7 - (a^{12} - a^6 + 1)t^6 - a^{12}t^5 + (a^6 - 1)t^4 - a^{12}t^3 - (a^{12} - a^6 + 1)t^2 - t + 1$. Also in this case, $f(1) = -a^{12}$ and $f(-1) = 1$. If $p \neq 3$, the product $y\tau$ should have trace 0, in contrast with $\mathrm{tr}(y\tau) = -16$. □

LEMMA 6.4. *Assume $a^2 \neq 3$. The group $K_{|S_9}$ is not contained in any maximal subgroup $M \cong \mathrm{PSL}_2(q).2$ or $M \cong \mathrm{PSL}_2(q^2).2$ in class $\mathcal{S}$ of $\Omega_9(q)$.*

PROPOSITION 6.5. *Assume q odd and $n \in \{12, 16, 20\}$. Let $a \in \mathbb{F}_q^*$ be such that $\mathbb{F}_p[a^2] = \mathbb{F}_q$ with $a^2 \neq 2, 3$. Then $K_{|S_9} = \Omega_9(q)$.*

PROOF. By Lemmas 6.1 and 6.3, $K_{|S_9}$ is absolutely irreducible and is neither contained in a maximal subgroup in class C_2 of $\Omega_9(q)$ nor contained in any maximal subgroup in class C_7. Furthermore, by Lemmas 6.2 and 6.4, either $K_{|S_9} = \Omega_9(q)$ or $K_{|S_9}$ is contained in a maximal subgroup $M \in \{\Omega_9(q_0), \mathrm{SO}_9(q_0)\}$ in class C_5, where $q = q_0^r$ for some prime $r \geq 2$. Suppose there exists $g \in \mathrm{GL}_9(\mathbb{F})$ such that $\tau^g = \tau_0$, $y^g = y_0$, with $\tau_0, y_0 \in \mathrm{GL}_9(q_0)$. From $\mathrm{tr}((y\tau)^2) = -2176a^4 + 6784a^2 - 224$ and $\mathrm{tr}((y^2\tau)^2) = 1920a^4 - 5504a^2 - 288$, we get that $-17a^4 + 53a^2$ and $15a^4 - 43a^2$ belong to $\mathbb{F}_{q_0}$, whence $64a^2 \in \mathbb{F}_{q_0}$. We conclude that $K_{|S_9} = \Omega_9(q)$. □

COROLLARY 6.6. *Assume q odd and $n \in \{12, 16, 20\}$. Let $a \in \mathbb{F}_q^*$ be such that $\mathbb{F}_p[a^2] = \mathbb{F}_q$ with $a^2 \neq 2, 3$. Then $H = \Omega_n^+(q)$. In particular, $\Omega_n^+(q)$ is $(2, 3)$-generated.*

PROOF. Since $K_{|S_9} = \Omega_9(q)$, we can repeat the argument of Corollary 5.6, proving that $H = \Omega_n^+(q)$. For the second part of the statement, we have to prove that there exists an element a satisfying all the hypotheses. If $q = p$, take $a = 1$. Suppose now $q = p^f$ with $f \geq 2$ and let $\mathcal{N}(q)$ be the number of elements $b \in \mathbb{F}_q^*$ such that $\mathbb{F}_p[b^2] \neq \mathbb{F}_q$. By [12, Lemma 2.7], it suffices to check that the condition $p^f - 2p(p^{\lfloor f/2 \rfloor} - 1)/(p-1) > 1$ is always fulfilled (the requirements $a^2 \neq 2, 3$ can be dropped). □

https://doi.org/10.1017/S1446788724000016 Published online by Cambridge University Press

7. Conclusions

We can now prove our main result.

PROOF OF THEOREM 1.1. The $(2,3)$-generation of $\Omega_n(q)$, nq odd, follows from Theorem 3.7 when $n \in \{9, 11, 13, 17\}$ and Corollary 5.6 for the other values of n. Due to Corollaries 5.6 and 6.6, we also proved the $(2,3)$-generation of the following even-dimensional orthogonal groups: $\Omega^+_{2k}(q)$, when $q \equiv 1 \pmod 4$ and $k = 6$ or $k \geq 8$; $\Omega^+_{4k}(q)$, when $q \equiv 3 \pmod 4$ and $k \geq 3$; $\Omega^-_{4k+2}(q)$, when $q \equiv 3 \pmod 4$ and $k \geq 4$. □

References

[1] J. N. Bray, D. F. Holt and C. M. Roney-Dougal, *The Maximal Subgroups of the Low-Dimensional Finite Classical Groups*, London Mathematical Society Lecture Note Series, 40 (Cambridge University Press, Cambridge, 2013).

[2] M. Cazzola and L. Di Martino, '$(2,3)$-generation of $PSp(4,q)$, $q = p^n$, $p \neq 2, 3$', *Results Math.* **23** (1993), 221–232.

[3] R. M. Guralnick and J. Saxl, 'Generation of finite almost simple groups by conjugates', *J. Algebra* **268** (2003), 519–571.

[4] C. S. H. King, 'Generation of finite simple groups by an involution and an element of prime order', *J. Algebra* **478** (2017), 153–173.

[5] P. Kleidman and M. Liebeck, *The Subgroup Structure of the Finite Classical Groups*, London Mathematical Society Lecture Note Series, 129 (Cambridge University Press, Cambridge, 1990).

[6] M. W. Liebeck and A. Shalev, 'Classical groups, probabilistic methods, and the $(2,3)$-generation problem', *Ann. of Math. (2)* **144** (1996), 77–125.

[7] M. A. Pellegrini, 'The $(2,3)$-generation of the classical simple groups of dimensions 6 and 7', *Bull. Aust. Math. Soc.* **93** (2016), 61–72.

[8] M. A. Pellegrini, 'The $(2,3)$-generation of the special linear groups over finite fields', *Bull. Aust. Math. Soc.* **95** (2017), 48–53.

[9] M. A. Pellegrini and M. C. Tamburini Bellani, 'The $(2,3)$-generation of the finite unitary groups', *J. Algebra* **549** (2020), 319–345.

[10] M. A. Pellegrini and M. C. Tamburini Bellani, 'On the $(2,3)$-generation of the finite symplectic groups', *J. Algebra* **598** (2022), 156–193.

[11] M. A. Pellegrini and M. C. Tamburini Bellani, 'The $(2,3)$-generation of the finite 8-dimensional orthogonal groups', *J. Group Theory* **26** (2023), 333–356.

[12] M. A. Pellegrini, M. C. Tamburini Bellani and M. A. Vsemirnov, 'Uniform $(2,k)$-generation of the 4-dimensional classical groups', *J. Algebra* **369** (2012), 322–350.

[13] M. C. Tamburini and J. S. Wilson, 'On the $(2,3)$-generation of some classical groups, II', *J. Algebra* **176** (1995), 667–680.

[14] M. C. Tamburini, J. S. Wilson and N. Gavioli, 'On the $(2,3)$-generation of some classical groups, I', *J. Algebra* **168** (1994), 353–370.

[15] D. E. Taylor, *The Geometry of the Classical Groups*, Sigma Series in Pure Mathematics, 9 (Heldermann Verlag, Berlin, 1992).

[16] M. A. Vsemirnov, 'On $(2,3)$-generated groups', in: *Group Theory Conference in Honour of V. Mazurov, Novosibirsk, 20th July 2013*, slides of the conference available at www.math.nsc.ru/conference/groups2013/slides/MaximVsemirnov_slides.pdf.

MARCO ANTONIO PELLEGRINI, Dipartimento di Matematica e Fisica,
Università Cattolica del Sacro Cuore,
Via della Garzetta 48, 25133 Brescia, Italy
e-mail: marcoantonio.pellegrini@unicatt.it

MARIA CHIARA TAMBURINI BELLANI, Dipartimento di Matematica e Fisica,
Università Cattolica del Sacro Cuore,
Via della Garzetta 48, 25133 Brescia, Italy
e-mail: mariaclara.tamburini@gmail.com