Groups Geom. Dyn. 1 (2007), 623–660

Groups, Geometry, and Dynamics

Extremely primitive groups

Avinoam Mann, Cheryl E. Praeger and Ákos Seress

Abstract. A primitive permutation group is called extremely primitive if a point stabilizer acts primitively on each of its orbits. We prove that finite extremely primitive groups are of affine type or almost simple. Moreover, we determine the affine type examples up to finitely many exceptions.

Mathematics Subject Classification (2000). 20B15.

Keywords. Primitive permutation groups.

1. Introduction

A primitive permutation group is called *extremely primitive* if a point stabilizer is primitive on each of its orbits (where we regard the trivial group acting on a set of size 1 as primitive). Extremely primitive groups were the subject of a 1927 paper of W. A. Manning [22], and interest again focused on them following efforts to extend the Bounded Subdegrees Theorem proved by G. Schlichting [26] in 1980 (and reproved by V. Trofimov in 1985, and G. M. Bergman and H. W. Lenstra in 1989, see [23]) concerning the structure of a transitive permutation group given a finite upper bound on its subdegrees. Extremely primitive groups are among the most natural primitive groups to be studied further, and examples of these include

(a) $G \cong Z_p$ acting regularly on $\Omega = G$ by right multiplication, where p is a prime, and

(b) each 2-primitive permutation group G on Ω; a classification of all such groups is available and depends on the finite simple group classification.

If a finite group G is extremely primitive and is not one of these examples, then G is not regular on Ω, since the only primitive regular permutation groups are cyclic of prime order. Also G is *simply primitive*, that is, G is not 2-transitive, since the only

The second and third authors wish their colleague Avinoam Mann a happy and productive retirement. This project forms part of an Australian Research Council Discovery Grant of the second author. The third author was partially supported by the NSA and NSF.

2-transitive examples are 2-primitive. Thus if we exclude these examples, then all finite extremely primitive groups G satisfy the following conditions.

(A) G is a simply primitive permutation group on a finite set Ω such that, for $\alpha \in \Omega$, the stabilizer $G_\alpha \neq 1$, and G_α acts primitively on each of its orbits in Ω.

These conditions may be stated in an equivalent form as follows (setting $H := G_\alpha$).

(A′) G is a finite group with a maximal non-trivial core-free subgroup H, such that $H \cap H^x$ is maximal in H, for each $x \in G \setminus H$, and there are at least three H-double-cosets.

It follows from an old result of Manning [22] (or see [30, 17.6]) that G_α is faithful on each of its orbits in $\Omega \setminus \{\alpha\}$. In the setting of (A′), Manning's result is that $H \cap H^x$ is core-free in H for each $x \in G \setminus H$. We study groups satisfying these conditions in an attempt to classify them, a problem that was mentioned in [23]. In that paper the authors considered transitive groups, not necessarily finite, with a point stabilizer acting primitively on each suborbit. As was explained there, the problem does not reduce to the case of primitive groups discussed here, but still that case seems a natural first step. We also confine ourselves to finite groups.

Our main results are as follows.

Theorem 1.1. *If $G \leq \mathrm{Sym}(\Omega)$ is extremely primitive then G is of affine type or almost simple.*

The bulk of this paper is the further analysis of the affine case. We shall return to the classification of extremely primitive groups of almost simple type in a sequel. The proof of Theorem 1.1 is independent of the finite simple group classification, but further results rely on this classification: namely Theorem 1.2 through its use of the classification of finite 2-transitive groups, and Theorem 1.3 where more detailed information about simple groups and their representations is needed.

Theorem 1.2. *Let $G \leq \mathrm{Sym}(\Omega)$ be extremely primitive of affine type, so that $|\Omega| = p^d$ for some prime p, $G = NH \leq \mathrm{AGL}(d, p)$ with $N = Z_p^d$ and H an irreducible subgroup of $\mathrm{GL}(d, p)$. Then one of the following holds.*

(a) (*Soluble examples*)

  (i) $d = 1$ *and* $H = 1$*; or*

  (ii) $H = Z_q$*, where q is a prime, and* $o(p \bmod q) = d$*; or*

  (iii) $H = Z_q.Z_e$*, with q as in* (ii)*, and e divides d.*

(b) (2-*transitive, insoluble examples*) $p = 2$ *and one of the following holds.*

  (i) $H = \mathrm{SL}(d, 2)$ *for* $d \geq 3$*, or* $H = \mathrm{Sp}(d, 2)$ *for* $d \geq 4$ *even;*

  (ii) $(d, H) = (4, A_6), (4, A_7), (6, \mathrm{PSU}(3, 3)), (6, \mathrm{PSU}(3, 3).2)$.

(c) (*Insoluble, simply primitive examples*) $p = 2$ *and* H *is almost simple.*

Moreover each of the groups in parts (a) *and* (b) *is extremely primitive.*

To classify the finite affine extremely primitive groups it remains to find all the examples in part (c) of Theorem 1.2. This we do up to a finite number of possibilities.

Theorem 1.3. *For the pairs* (d, H) *in* (a)–(c) *below, the group* $Z_2^d.H$ *is simply primitive and extremely primitive.*

(a) $\mathrm{Soc}(H)$ *sporadic:*
$(10, M_{12})$, $(10, M_{22})$, $(10, M_{22}.2)$, $(11, M_{23})$ (*two groups*), $(11, M_{24})$ (*two groups*), $(22, \mathrm{Co}_3)$, $(24, \mathrm{Co}_1)$;

(b) $\mathrm{Soc}(H)$ *alternating:*
$(2k, A_{2k+1})$, $(2k, S_{2k+1})$ *for* $k \geq 2$, $(2k, A_{2k+2})$, $(2k, S_{2k+2})$ *for* $k \geq 3$;

(c) $\mathrm{Soc}(H)$ *of Lie type:*
$(2k, \Omega^{\pm}(2k, 2))$, $(2k, \Omega^{\pm}(2k, 2).2)$ *for* $k \geq 3$, $(8, \mathrm{PSL}(2, 17))$, $(8, \mathrm{Sp}(6, 2))$.

Moreover, there are only finitely many insoluble, simply primitive, extremely primitive groups of affine type not occurring on this list.

Note that up to permutational isomorphism there are two extremely primitive groups with structure $Z_2^{11}.M_{23}$ and also there are two such groups with structure $Z_2^{11}.M_{24}$. We conjecture that the list in Theorem 1.3 is complete. We say more about this conjecture in Subsection 4.1. In particular, modulo a proof of a conjecture of G. E. Wall, the only possible additional examples are for the pairs $(d, \mathrm{Soc}(H))$ listed in Table 2 (see Theorem 4.8).

We prove Theorem 1.1 in Section 2, Theorem 1.2 in Section 3, and Theorem 1.3 in Section 4.

2. Reduction to the affine and almost simple cases

In this section we prove Theorem 1.1. If $G \leq \mathrm{Sym}(\Omega)$ is either cyclic of prime order or 2-transitive, then it is primitive of affine or almost simple type and there is nothing to prove. Hence it is enough to consider the case when G, Ω, and $H := G_\alpha$ satisfy condition (A), or equivalently, condition (A$'$).

Let N be a minimal normal subgroup of G. Then N is transitive on Ω and hence $G = NH$. The various possibilities for the structure of N and H are described by the O'Nan–Scott Theorem [4, 4.1A]. First we treat the case where N is regular on Ω.

Lemma 2.1. *If* N *is regular on* Ω, *that is, if* $N \cap H = 1$, *then* N *is elementary abelian, and hence Theorem* 1.1 *holds.*

Proof. We may identify N with Ω, so that N acts on itself by right multiplication, and H acts on N by conjugation. Thus if $1 \neq x \in N$ and $h \in H \cap H^x$, then $h = h_1^x$ for some $h_1 \in H$, so $[h_1, x] = h_1^{-1}h \in H \cap N = 1$. Hence $h_1 \in C_H(x)$, implying that $h = h_1$, and that $C_H(x) = H \cap H^x$. Therefore, $C_H(x)$ is maximal in H. Note that $C_H(x) \neq H$, because H fixes only one point of Ω.

Suppose that N is not elementary abelian. Then N is not nilpotent, G is not a Frobenius group (see [30, Theorem 5.1′]), and therefore some non-identity element $u \in \Omega = N$ is fixed by some non-identity element of H. Thus $C_H(u) \neq 1$, and it follows that H is not of prime order. Then, for any $x \in N^\#$, the stabilizer $C_H(x)$ of x in H is maximal in H, and hence $C_H(x) \neq 1$.

Let $K_1, \ldots, K_r$ be the distinct subgroups of H occurring as centralizers of non-identity elements of N, with $K_i = C_H(x_i)$, say, and let $C_i = C_N(K_i)$. Now each element of N lies in at least one of the subgroups C_i. If $i \neq j$, then $\langle K_i, K_j \rangle = H$ since K_i, K_j are maximal in H and so $C_i \cap C_j$ centralizes $\langle K_i, K_j \rangle = H$. Hence $C_i \cap C_j = 1$. Thus the ${C_i}^\# = C_1 \setminus \{1\}$ form a partition of $N^\#$. The insoluble groups with a partition were determined by M.Suzuki [28], and are the groups $\mathrm{PSL}(2, q)$, $\mathrm{Sz}(q)$, and $\mathrm{PGL}(2, q)$. Here N must be one of the first two as it is minimal normal in G. If N is the unique minimal normal subgroup of G, then G is almost simple. Otherwise G has exactly two minimal normal subgroups, which are isomorphic simple groups, say N_1 and N_2, two copies of the simple group N. Let $S = N_1 \times N_2$, the socle of G. Then we may assume that $H \cap S$ is the diagonal subgroup $D = \{(x, x) \mid x \in N\}$. Since H is primitive on the G-conjugacy classes contained in N_1, and $D \lhd H$, D is transitive on the same classes, which means that the G-classes are N_1-classes. However, an outer automorphism of a non-abelian simple group moves some conjugacy class [5, Theorem C], and therefore G induces only inner automorphisms on N_1, which in turn means that $G = N_1 C_G(N_1) = S$ and $H = D$. However if $x \in N_1$ is a non-identity element of prime order p, where p divides q, then $C_H(x) = \{(y, y) \mid y \in C_N(x)\}$ is not maximal in H, which is a contradiction. □

Thus we may assume that G has no regular minimal normal subgroups. By Theorem [4, 4.1A], G has a unique minimal normal subgroup $N = T_1 \times \cdots \times T_k$, where the T_i are all isomorphic to a non-abelian simple group T, and $k \geq 1$. We show next that G does not preserve a non-trivial Cartesian decomposition of the point set Ω.

Lemma 2.2. *There is no non-trivial decomposition $\Omega = \Sigma^l$ $(l \geq 2)$ such that $G \leq \mathrm{Sym}(\Sigma) \wr S_l$ in product action.*

Proof. Suppose that $\Omega = \Sigma^l$ $(l \geq 2)$ and $G \leq \mathrm{Sym}(\Sigma) \wr S_l$ in product action. Since N is non-abelian and non-regular, it follows from [14, 2.4] that, replacing G by a conjugate in $\mathrm{Sym}(\Sigma) \wr S_l$ if necessary, we may assume that $G \leq L \wr S_l$ where L is a primitive subgroup of $\mathrm{Sym}(\Sigma)$ and $N = \mathrm{Soc}(L)^l$. Thus $\mathrm{Soc}(L) \cong T^m$ where

$k = lm$. Since $G = NH$, the subgroup H is transitive on both the k simple direct factors of N, and the l entries of points of Σ^l.

We may take the point $\alpha \in \Omega$ to be $\alpha = (\sigma, \ldots, \sigma)$ for some $\sigma \in \Sigma$. Then $H = G_\alpha \leq (L \wr S_l)_\alpha = L_\sigma \wr S_l$. In particular, $N_\alpha = (\mathrm{Soc}(L_\sigma))^l$, and since N is not regular, $N_\alpha \neq 1$. Let Δ be an orbit for H in $\Omega \setminus \{\alpha\}$. Then $N_\alpha = N \cap H$ is a nontrivial normal subgroup of H, and as H acts faithfully and primitively on Δ, it follows that $N \cap H$ is transitive on Δ. Hence H and $N \cap H$ have the same orbits in Ω. Now the set $\{(\tau, \sigma, \sigma, \ldots, \sigma) \mid \tau \in \Sigma\} = \Sigma \times \{\sigma\}^{l-1}$ is clearly invariant under the action of $N \cap H$, and hence is a union of orbits of $N \cap H$. However as H acts transitively on the entries of points of Σ^l, and $H \leq L_\sigma \wr S_l$, this subset is not invariant under the action of H, and hence is not a union of H-orbits. □

It follows from Lemma 2.2 and the O'Nan–Scott Theorem (see [19]) that, if G has no regular normal subgroup, and G does not preserve a non-trivial Cartesian decomposition of Ω, then either G is almost simple, or G has simple diagonal type. Thus in order to complete the proof of Theorem 1.1, it is sufficient to show that G does not have simple diagonal type. Suppose to the contrary that it does. Then, replacing G by a conjugate if necessary, we may assume that G is a subgroup of the group W defined by

$$W = \left\{ (a_1, \ldots, a_k) \cdot \pi \;\middle|\; \begin{array}{l} a_i \in \mathrm{Aut}(T), \pi \in S_k, \\ a_i \equiv a_j \pmod{\mathrm{Inn}(T)} \end{array} \text{ for all } i, j \right\}$$

where $\pi^{-1}(a_1, \ldots, a_k)\pi = (a_{1\pi^{-1}}, \ldots, a_{k\pi^{-1}})$. The socle of W is the group $\mathrm{Soc}(W) = \{(t_1, \ldots, t_k) \mid t_i \in \mathrm{Inn}(T)\}$, the set $\Omega = T^{k-1}$, and W acts on Ω as follows:

$$\begin{aligned} (a_1, \ldots, a_k)\colon\ & (t_1, \ldots, t_{k-1}) \mapsto (a_k^{-1} t_1 a_1, \ldots, a_k^{-1} t_{k-1} a_{k-1}) \qquad \text{and} \\ \pi\colon\ & (t_1, \ldots, t_{k-1}) \mapsto (t_{k\pi^{-1}}^{-1} t_{1\pi^{-1}}, \ldots, t_{k\pi^{-1}}^{-1} t_{(k-1)\pi^{-1}}) \end{aligned}$$

for $(a_1, \ldots, a_k)\pi \in W$ and $(t_1, \ldots, t_{k-1}) \in T^{k-1}$, where $t_k = 1_T$. Thus for $\alpha = (1_T, \ldots, 1_T) \in T^{k-1}$, $W_\alpha = A \times S_k$ where $A = \{(a, \ldots, a) \mid a \in \mathrm{Aut}(T)\}$. A subgroup G of W containing N is primitive on Ω provided that G acts primitively on the simple direct factors of N. Since $G = NH$ we have that H acts primitively on these simple direct factors.

Lemma 2.3. *If G is of simple diagonal type, then $k = 2$ and, for each $t \in T$, $t \neq 1$, there is an automorphism $a(t) \in \mathrm{Aut}(T)$ which inverts t such that $a(t)^2 \in \mathrm{Inn}(T)$, and $\langle C_{\mathrm{Inn}(T)}(t), a(t)\rangle$ is a maximal subgroup of $\langle \mathrm{Inn}(T), a(t)\rangle$. Moreover, $\langle \mathrm{Inn}(T), a(t)\rangle$ is independent of $t \in T \setminus \{1\}$.*

Proof. Suppose that G is a subgroup of the group W defined above. Consider the point $\delta = (t, 1, \ldots, 1) \in \Omega = T^{k-1}$, where $t \in T, t \neq 1$. The N_α-orbit containing δ

is the set $\{(t^x, 1, \ldots, 1) \mid x \in T\}$, which in particular has size greater than 1. Let Δ denote the H-orbit containing δ. Since the normal subgroup N_α of H acts nontrivially on Δ, and since H is primitive on Δ it follows that $\Delta = \{(t^x, 1, \ldots, 1) \mid x \in T\}$. However, since H is transitive on the simple direct factors of N, it follows from the definition of the action that, when $k \geq 3$, the H-orbit containing δ contains a $(k-1)$-tuple with non-trivial second entry.

Therefore $k = 2$, so $\Omega = T$ and Δ is the conjugacy class containing t. We have $N_\alpha \leq H \leq \mathrm{Aut}(T) \times \langle \tau \rangle$ where $\langle \tau \rangle = S_2$ and $\tau \colon x \mapsto x^{-1}$ for all $x \in T$. Now $H \cap \mathrm{Aut}(T)$ must leave the H-orbit Δ invariant, and it follows that $H \cap \mathrm{Aut}(T)$ leaves all conjugacy classes of T invariant. Since for each outer automorphism of a non-abelian simple group T there is a conjugacy class of T which it moves [5, Theorem C], it follows that $H \cap \mathrm{Aut}(T) = \mathrm{Inn}(T) = N_\alpha$, and $|H : N_\alpha| \leq 2$.

Now H contains an element which interchanges the two simple factors of N, so $|H : N_\alpha| = 2$. Such an element is of the form $a\tau$ for some $a \in \mathrm{Aut}(T)$, and $a\tau \colon t \mapsto (t^a)^{-1}$. Since N_α is transitive on Δ we have $H = N_\alpha H_\delta$, so we may assume in addition that $a\tau \in H_\delta$. Therefore $t^a = t^{-1}$, and hence every element t of T is mapped to its inverse by some automorphism $a = a(t)$. Also $(a\tau)^2 = a^2 \in H \cap \mathrm{Aut}(T) = \mathrm{Inn}(T)$. Now $H = \langle \mathrm{Inn}(T), a\tau \rangle$, and $H_\delta = \langle C_{\mathrm{Inn}(T)}(t), a\tau \rangle$ is a maximal subgroup of H. Moreover $H \leq W_\alpha = A \times S_k$, and H projects faithfully onto A with image $\langle \mathrm{Inn}(T), a \rangle$. It follows that $\langle C_{\mathrm{Inn}(T)}(t), a \rangle$, the image of H_δ under this projection, is a maximal subgroup of $\langle \mathrm{Inn}(T), a \rangle$, and that $\langle \mathrm{Inn}(T), a \rangle$ is independent of the choice of t in $T \setminus \{1\}$. □

We now prove that there are no simple groups satisfying the conditions of Lemma 2.3, thereby completing the proof of Theorem 1.1.

Lemma 2.4. *There is no simple group satisfying the conditions on the group T given in Lemma* 2.3.

Proof. Let T be a finite non-abelian simple group, and identify T with the subgroup $\mathrm{Inn}(T)$ of its automorphism group $\mathrm{Aut}(T)$. Suppose that T satisfies the conditions of Lemma 2.3, that is, there is a subgroup A of $\mathrm{Aut}(T)$, containing T as a subgroup of index at most 2, such that, for each $t \in T$, $t \neq 1$, there exists $a(t) \in A$ with $t^{a(t)} = t^{-1}$, $a(t)^2 \in T$, and $\langle C_T(t), a(t) \rangle$ maximal in A. Note that $a(t)$ normalizes $C_T(t)$, and that $|C_T(t)\langle a(t) \rangle : C_T(t)| \leq 2$. Index 1 occurs if and only if t is an involution and $a(t) \in T$, that is, $A = T$. In any case, $C_T(t)$ is normal in $C_T(t)\langle a(t) \rangle$.

Let t be an involution, and assume that some non-identity element $x \in C_T(t)$ has odd order. Then both t and x are powers of tx. Also $a(tx)$ inverts x and fixes t, and $C_T(tx)$ fixes both x and t. Hence $\langle C_T(xt), a(xt) \rangle \leq \langle C_T(t), a(t) \rangle = C_A(t)$ and $C_T(tx) \leq C_T(x)$. The maximality condition of Lemma 2.3 implies that $\langle C_T(tx), a(tx) \rangle = C_A(t)$. It follows that x centralizes a subgroup of $C_T(t)$ of index at most 2, and therefore all elements of odd order in $C_T(t)$ lie in $Z(O^2(C_T(t)))$ (where

$O^2(C_T(t))$ is the smallest normal subgroup of $C_T(t)$ with quotient a 2-group). Thus the set consisting of all these elements forms a normal 2-complement in $C_T(t)$. By D. Gorenstein's characterization [7] of groups of this type, T is one of the simple groups $\mathrm{PSL}(2,q)$, $\mathrm{Sz}(q)$, $\mathrm{PSL}(3,4)$, or A_7.

If T is one of $\mathrm{PSL}(n,q)$ or $\mathrm{Sz}(q)$, let t be an element of order p, where p is the defining characteristic. In A_7, let $t = (123)(456)$. Write $C = C_T(t)$. Since $\langle C, a(t)\rangle \le N_A(C)$, the maximality implies equality, and $|N_A(C) : C| \le 2$. For these groups, this is only possible if $A = T = \mathrm{PSL}(2,5)$, but for this group the condition fails on taking t to be an involution. □

3. Affine groups

In this section we prove Theorem 1.2. Throughout this section we shall assume that G is extremely primitive of affine type, and is not regular of prime order. Thus we have $G = NH$, where $N = Z_p^d$ and H is a non-trivial irreducible subgroup of $\mathrm{GL}(d,p)$, for some prime p and positive integer d. The centralizer of H in $\mathrm{GL}(d,p)$ is therefore isomorphic to $\mathrm{GF}(p^a)^\#$, for some integer a dividing d (possibly $a = 1$). We may, and shall, assume that $H \le \mathrm{GL}(d/a, p^a)\cdot a$, and identify N with the additive group of a (d/a)-dimensional vector space V over the field $F = \mathrm{GF}(p^a)$. The integer a is the largest for which such an embedding is possible. Further we identify $\Omega = V$, with N and H acting naturally. First we examine elements of H which fix some 1-dimensional subspace of Ω.

Lemma 3.1. *If $h \in H$ and $v \in \Omega$ are such that $v^h = \lambda v$ for some $\lambda \in F$, then $\lambda = 1$ (that is, 1 is the only possible eigen-value for an element of H). In particular, H contains no non-identity element of order dividing $p^a - 1$.*

Proof. Suppose that $0 \ne v \in \Omega$ and $h \in H$ are such that v^h lies in the F-space $\langle v\rangle_F$ spanned by v. Then $\langle v^h\rangle_F = \langle v\rangle_F$. Moreover, identifying v with the corresponding element of N, we have that $C_H(v)^h = C_H(v^h)$ fixes each element of $\langle v^h\rangle_F = \langle v\rangle_F$, and it follows that $C_H(v)^h = C_H(v) = H \cap H^v$. By condition (A), $H \cap H^v$ is maximal in H, and since h normalizes $C_H(v) = H \cap H^v$, it follows that $h \in C_H(v)$, and therefore $v^h = v$. Thus 1 is the only possible F-eigen-value for any element of H. However, if the order of h divides $p^a - 1$, then all the eigen-values of h (in its splitting field) lie in F, and it follows that the only such element is $h = 1$. □

We now consider the actions of normal subgroups of H, and then we deal with soluble extremely primitive groups.

Lemma 3.2. *If M is a non-trivial normal subgroup of H, then M and H have the same orbits in Ω, and M leaves invariant no proper non-trivial subgroup of N.*

Proof. As in the proof of Lemma 2.1, we denote by $K_1, \dots, K_s$ the distinct intersections $H \cap H^x = C_H(x)$, for $x \in N^\#$. Then by Condition (A), each K_i is a maximal subgroup of H. The fact that H is faithful on each of its orbits implies that M is not contained in any K_i, so $H = MK_i$ for each i. This is equivalent to the assertion that M is transitive on each H-orbit in $\Omega \setminus \{0\}$. Suppose that L is a non-identity M-invariant subgroup of N, and let $1 \neq x \in L$. Because H is primitive on the H-orbit x^H containing x, M is transitive on x^H, and hence this orbit is contained in L. Thus L is H-invariant, so $L = N$. □

Lemma 3.3. *If G is soluble and extremely primitive, then part* (a) *of Theorem* 1.2 *holds.*

Proof. If $H = 1$ then case (a) (ii) of Theorem 1.2 holds, so we may take $H \neq 1$ (as assumed for this section). Let M be a minimal normal subgroup of H. By Lemma 3.2, M is transitive on each H-orbit. Since H is soluble, M is elementary abelian, and since a transitive abelian permutation group is regular, it follows that M induces a regular permutation group on each H-orbit in $\Omega \setminus \{0\}$. Then since H, and hence also M, acts faithfully on each such H-orbit, it follows that each of these H-orbits has length $|M|$. Hence G is a soluble 3/2-transitive group. These groups were determined by Passman [24, 25]. The examples are divided into four categories, and we consider each category in turn, to determine which of the soluble 3/2-transitive groups satisfy Condition (A).

1. *G is a Frobenius group.* In this case N is the Frobenius kernel and H is a Frobenius complement. The intersections $H \cap H^x$ ($x \in N^\#$) are trivial, so H is primitive and regular on each of its orbits in $\Omega \setminus \{0\}$. Thus H has prime order, say q. The maximality of H in G is equivalent to N being a minimal normal subgroup, so G is as in case (a) (ii) of Theorem 1.2.

2. $G \leq A\Gamma L(1, p^d)$. Here $H \leq \Gamma L(1, p^d)$, so H is metacyclic, and if the cyclic normal subgroup $T = H \cap GL(1, p^d)$ is trivial, then H is cyclic. Choosing M, in the argument above, to be a subgroup of T if $T \neq 1$, then M has prime order, q say, and we see that each H-orbit in $\Omega \setminus \{0\}$ has length q, and that M is transitive on it. If $T = 1$, then $H = M$, and case (a) (ii) of Theorem 1.2 holds. If $T \neq 1$, then T is faithful and transitive on each of the H-orbits and hence $|T| = q$. If T is contained in $GL(1, p^b)$, for some proper subfield $GF(p^b)$ of F, then this subfield constitutes a proper H-invariant subgroup of N, contradicting the maximality of H in G. Thus T is contained in no such subgroup, which means that NT is as in case (a) (ii) of Theorem 1.2. In this case, we may identify Ω with the additive group of the field F. Let $K = K_1$ be the stabilizer in H of the multiplicative identity 1 of $F = \Omega$. Then we have $K \cap T = 1$, and K is a subgroup of the Galois group of F. If $K = 1$ then $G = NT$ is as in case (a) (ii) of Theorem 1.2, while if $K \neq 1$, then K is cyclic of order e, where e divides d, and G is as in case (a) (iii) of Theorem 1.2.

3. *$G \le A\Gamma L(2,q)$, where $q = p^{d/2}$ with d even, $H \le \Gamma L(2,q)$, and $H \cap GL(2,q)$ consists of diagonal or anti-diagonal matrices of determinant* 1 *or* -1. (By an anti-diagonal matrix we mean one whose nonzero entries are all on the northeast to southwest diagonal.) In this case H is the union of diagonal and anti-diagonal matrices, and so it is a dihedral group of order $2q$, say. Its cyclic subgroup T of index 2 acts faithfully and transitively on each of the H-orbits in $\Omega \setminus \{0\}$. Therefore, for each $x \in N^{\#}$, $H \cap H^x$ has order 2, and since $H \cap H^x$ is maximal in H it follows that q is prime. Again G is as in case (a) (iii) of Theorem 1.2, with $e = 2$.

4. *G is one of several exceptional groups, of degrees* 3^2, 5^2, 7^2, 11^2, 17^2, *or* 3^4. We will show that this case does not lead to new examples. First, Lemma 3.1 shows that $|H|$ is odd. Since all H-orbits in $\Omega \setminus \{0\}$ have equal size, the indices $|H : H \cap H^x|$ ($x \in N^{\#}$) divide $p^d - 1$. The only possible odd divisors are 3, 5, 15, and 9. Here 15 is impossible, because the index of a maximal subgroup in a soluble group is a prime-power. If the index is 3 or 5, then H is isomorphic to a subgroup of odd order of either S_3 or S_5, and it follows that H itself has order 3 or 5 respectively. Then considering a minimal normal subgroup of G the maximality of H implies that G is as in case (a) (ii) of Theorem 1.2. Finally let the index be 9. Then $|N| = 17^2$, and since H acts faithfully as a soluble and primitive permutation group of degree 9, H contains a normal elementary abelian subgroup of order 9. However, $H \le \Gamma L(2,17)$, which has no elementary abelian subgroup of order 9. □

For the rest of this section we therefore assume that H is insoluble. First, we verify that the list of 2-transitive extremely primitive groups in Theorem 1.2 is correct.

Lemma 3.4. *If $G = Z_p^d.H$ is insoluble and 2-transitive, then part* (b) *of Theorem* 1.2 *holds.*

Proof. The 2-transitive affine permutation groups G are known (see e.g. [2, Table 7.3]) and more details on the structure of H can be found in [17, Appendix]. There are three infinite families, with H containing a normal subgroup isomorphic to one of the following three types: $SL(d/a, p^a)$ for some $a \le d/2$, $Sp(d/a, p^a)$ for some $a \le d/4$, or $G_2(p^a)'$ for $p = 2$ and $a = d/6$. There are also eleven sporadic examples with $2^4 \le p^d \le 59^2$. If H belongs to one of the three infinite families then H contains elements of order $p^a - 1$ and so, by Lemma 3.1, we have $p^a = 2$. This leads to the examples $H = SL(d,2)$, $Sp(d,2)$, $Sp(4,2)' \cong A_6$, $G_2(2)' \cong PSU(3,3)$, and $G_2(2) \cong PSU(3,3).2$ listed in Theorem 1.2 (b) (in the last two cases, we constructed H in *GAP* [6] to verify that H acts primitively on $\Omega \setminus \{\alpha\}$). Out of the eleven sporadic examples, in eight cases H does not have a faithful primitive representation (either $Soc(H)$ is not the product of isomorphic simple groups, or $|Soc(H)| = 2$). The remaining three cases are $G = Z_3^6.SL(2,13)$, $Z_{11}^2.SL(2,5)$, and $Z_2^4.A_7$. Lemma 3.1 eliminates the first two of these and the third one leads to an example listed in Theorem 1.2 (b). □

Finally, suppose that G is uniprimitive and H is insoluble. There are two types of information affecting the structure of H. On the one hand, H is an absolutely irreducible subgroup of $\mathrm{GL}(d/a, p^a).a$, and we have available the Aschbacher classification [1] of such subgroups to provide a framework for our investigation. On the other hand, H acts faithfully as a primitive permutation group on each of its orbits in $\Omega \setminus \{0\}$, and the O'Nan–Scott Theorem (see [19]) therefore provides information about the possible structure of H. We use a combination of these methods to complete the proof of Theorem 1.2. First we exploit the fact that H is primitive on each of its orbits in $\Omega \setminus \{0\}$ to prove that H has a unique minimal normal subgroup which is non-abelian.

Lemma 3.5. *If G is insoluble, then $p = 2$, and H has a unique minimal normal subgroup M, and M is nonabelian.*

Proof. If p were odd, then by Lemma 3.1, $|H|$ would be odd also, and hence G would be soluble, which is not the case. Hence $p = 2$. Let M be a minimal normal subgroup of H. By Lemma 3.2, each H-orbit is also an M-orbit. Suppose that M is regular on each non-trivial orbit of H. Then all these orbits have length $|M|$, and hence $|M|$ divides $|\Omega| - 1 = 2^d - 1$. Thus $|M|$ is odd, and so M is soluble, and hence is elementary abelian. Also, since H is faithful of each non-trivial orbit, M is self-centralizing in H. By Lemma 3.2, M leaves invariant no non-trivial proper subgroup of N. Hence M is an abelian irreducible group on N, and therefore M is cyclic. Then H/M, which is isomorphic to a group of automorphisms of M, is abelian and H is soluble, which is a contradiction. Thus M is not regular on some H-orbit, and because H is faithful and primitive on that orbit, it follows (see [19]) that M is not abelian and is the unique minimal normal subgroup of H. □

We now apply the Aschbacher classification [1] of subgroups of $\mathrm{GL}(d, p)$ to complete the proof of Theorem 1.2. We use the notation $\mathcal{C}_1$–$\mathcal{C}_8$, $\mathcal{S}$ of [13] to denote the categories of this classification. Recall that $H \leq \mathrm{GL}(d/a, p^a).a$ and a is maximal with respect to this property. We view H as acting semi-linearly on $V = \mathrm{GF}(p^a)^{d/a}$. By Lemma 3.5, $p = 2$ and H has a unique minimal normal subgroup M that is non-abelian.

Let $H_0 := H \cap \mathrm{GL}(d/a, 2^a)$. If $H_0 \geq \mathrm{SL}(d/a, 2^a)$, or H_0 contains a classical group of dimension d/a over $\mathrm{GF}(2^a)$, then Lemma 3.5 implies that H_0 is almost simple, satisfying the conclusion of Theorem 1.2 (c), and moreover in this case $M = \mathrm{Soc}(H)$ is absolutely irreducible on V. Thus we may assume that H_0 is contained in $\mathrm{GL}(d/a, 2^a).a$, or a general symplectic, general unitary or general orthogonal group of dimension d/a over $\mathrm{GF}(2^a)$, but neither contains the socle mod scalars of this group, nor leaves invariant any additional nondegenerate form. Then [1] implies that H_0 is in category $\mathcal{C}_i$ for some $i \leq 7$, or in category $\mathcal{S}$, for this group. If H_0 is in $\mathcal{S}$, then by Lemma 3.5, H_0 is almost simple, satisfying the conclusion of Theorem 1.2 (c), and by [1], $\mathrm{Soc}(H)$ is absolutely irreducible on V. Thus we have the following.

Lemma 3.6. *If H is insoluble and simply primitive, then either*

(a) *H is almost simple satisfying Theorem* 1.2 (c)*, not realisable over a proper subfield, and* $\mathrm{Soc}(H)$ *is absolutely irreducible on* $V = \mathrm{GF}(2^a)^{d/a}$*, or*

(b) *H_0 is in category $\mathcal{C}_i$ for some $i \in \{1, 2, \ldots, 7\}$.*

We may therefore assume that H_0 is in category $\mathcal{C}_i$ where $1 \le i \le 7$. By Lemma 3.2, H_0 leaves invariant no proper GF(2)-subspace of V. Hence H_0 is not a $\mathcal{C}_1$-subgroup. Moreover, since H_0 is irreducible on V, the maximality of a implies that H_0 is not a $\mathcal{C}_3$-subgroup of $\mathrm{GL}(d/a, 2^a)$ and in particular H_0 is absolutely irreducible on V, considered as a $\mathrm{GF}(2^a)$-vector space. Suppose that there is a proper subfield $\mathrm{GF}(q)$ of $\mathrm{GF}(2^a)$ such that H_0 is conjugate in $\mathrm{GL}(d/a, 2^a)$ to a subgroup of $Z \circ \mathrm{GL}(d/a, q)$, where Z is the subgroup of scalar matrices in $\mathrm{GL}(d/a, 2^a)$. Then H_0 leaves invariant a GF(2)-subspace of V of order at most $(2^a/q)q^{d/a} < 2^d$, contradicting Lemma 3.2. Thus the representation of H_0 is realizable over no proper subfield of $\mathrm{GF}(2^a)$ (that is, H_0 is not in category $\mathcal{C}_5$). Also, by Lemma 3.5, it follows that H_0 is not contained in the normalizer of a symplectic type r-group, where d/a is a power of the prime r (category $\mathcal{C}_6$). It therefore follows from [1] that either Theorem 1.2 (c) holds, or we have one of the following.

(i) H_0 leaves invariant a direct sum decomposition $\Omega = U_1 \oplus \cdots \oplus U_t$ where each U_i is a $\mathrm{GF}(2^a)$-subspace of dimension d/at, $t > 1$, and H_0 acts transitively on $\{U_1. \ldots, U_t\}$ (category $\mathcal{C}_2$).

(ii) H_0 leaves invariant a tensor product decomposition $\Omega = U \otimes W$ where U, W are $\mathrm{GF}(2^a)$-subspaces with $\dim U = m > 1$, $\dim W = n > 1$, and $d/a = nm$ (category $\mathcal{C}_4$).

(iii) H_0 leaves invariant a tensor imprimitivity system $\Omega = U_1 \otimes \cdots \otimes U_t$, such that each U_i is a $\mathrm{GF}(2^a)$-subspace of dimension $m > 1$, $d/a = m^t > m$, and H_0 acts transitively on $\{U_1. \ldots, U_t\}$ (category $\mathcal{C}_7$).

In the next lemmas we prove that none of the cases (i)–(iii) holds, thereby completing the proof of Theorem 1.2.

Lemma 3.7. *Case* (i) *above does not hold.*

Proof. Suppose that (i) holds and let u be a non-zero vector in U_1. By Lemma 3.2, M, H_0, H have the same orbits in Ω. Let Δ denote the H-orbit containing u. Then $U_1 \cap \Delta$ is a block of imprimitivity for the action of H on Δ. Since H_0 permutes the U_i transitively, $U_1 \cap \Delta$ is a proper subset of Δ, and since H is primitive on Δ it follows that $U_1 \cap \Delta = \{u\}$. This means that the sum v of the vectors in Δ is a non-zero vector which is left invariant by H, contradicting the fact that H is irreducible on Ω. □

Lemma 3.8. *Case* (ii) *above does not hold.*

Proof. Suppose that (ii) holds, and let u, w be non-zero vectors in U, W respectively. Let Δ denote the H-orbit containing $u \otimes w$. Then H acts primitively on Δ. Set $U \otimes w := \{z \otimes w \mid z \in U^\#\}$. Then $\Delta \cap (U \otimes w)$ contains $u \otimes w$ and is a block of imprimitivity for H in Δ. Moreover, $\Delta \cap (U \otimes w)$ is not equal to Δ, for if it were then H, in its induced action on W, would fix $\langle w \rangle_F$, whereas H is irreducible on W and $\dim W > 1$. It follows that $\Delta \cap (U \otimes w) = \{u \otimes w\}$. Now the stabilizer K in H of the 1-space $\langle w \rangle_F$ is equal to the setwise stabilizer in H of $U \otimes w$. From what we have just shown, K fixes $\Delta \cap (U \otimes w) = \{u \otimes w\}$. Thus $K = H_{\langle u \rangle_F}$. Since u was any non-zero vector in U, it follows that K fixes each 1-space $\langle u' \rangle_F$, $u' \in U^\#$. Thus K acts on U as a subgroup of scalar matrices, and similarly $K = H_{\langle u \rangle_F}$ acts on W as a subgroup of scalar matrices. Since, by Lemma 3.1, the only eigen-value for elements of H is 1, it follows that $K = 1$. Thus H acts faithfully, regularly and primitively on Δ, whence H is cyclic. This contradicts the assumption that H is insoluble. □

The proof that case (iii) does not hold is rather more delicate. We first standardise the representation of such groups.

Lemma 3.9. *Suppose that case* (iii) *above holds. We may identify each of the* U_i *with an* m*-dimensional* $\mathrm{GF}(2^a)$*-vectorspace* U *in such a way that* $H \le (\mathrm{GL}(U) \circ \cdots \circ \mathrm{GL}(U)).S_t$*, where* $\circ$ *denotes the central product. Let* K *denote the subgroup of* $\mathrm{GL}(U)$ *induced on* $U = U_1$ *by the stabilizer* H_1 *in* H *of the first tensor factor* U_1*. Then, replacing* H *by a conjugate under* $\mathrm{GL}(U) \circ \cdots \circ \mathrm{GL}(U)$ *if necessary, we may assume that* $H \le (N_{\mathrm{GL}(U)}(K) \circ \cdots \circ N_{\mathrm{GL}(U)}(K)).S_t$ *and* $H \cap (\mathrm{GL}(U) \circ \cdots \circ \mathrm{GL}(U)) \le K \circ \cdots \circ K$*.*

Proof. We work with the preimage of H in $\mathrm{GL}(U) \wr S_t$. By definition, $K = K_1$ is the set of all $h_1 \in \mathrm{GL}(U)$ such that there exists $(h_1, h_2, \ldots, h_t)\pi \in H$ with $1\pi = 1$. The subgroups K_j ($j \le t$) of $\mathrm{GL}(U)$ induced on $U_j = U$ by the stabilizer H_j in H of the j^{th} tensor factor U_j are defined similarly.

Let $x\rho \in H$, where $x = (x_1, \ldots, x_t) \in \mathrm{GL}(U)^t$ and $\rho \in S_t$, and suppose that $i\rho = j$. We claim that $K_i^{x_i} = K_j$. Let $k \in K_i$. There exists $h\pi \in H$ such that $h_i = k$ and $i\pi = i$. Then $(h\pi)^{x\rho} \in H$, and

$$(h\pi)^{x\rho} = h^{x\rho} \cdot (x^{-1})^\rho \cdot (x)^{\pi^{-1}\rho} \cdot \pi^\rho = x'\pi^\rho.$$

Now $(j)\pi^\rho = j$, and the j^{th} entry of x' is equal to the i^{th} entry of $h^x \cdot x^{-1} \cdot x^{\pi^{-1}}$, and this is $h_i^{x_i} x_i^{-1} x_i = h_i^{x_i} = k^{x_i}$. Hence $k^{x_i} \in K_j$, and so $K_i^{x_i} \subseteq K_j$. Similarly, since $(x\rho)^{-1} = (x^{-1})^\rho \rho^{-1} \in H$ and $j\rho^{-1} = i$, we have that $K_j^{x_i^{-1}} \subseteq K_i$. Hence $K_i^{x_i} = K_j$, as claimed.

Since H is transitive on $\{U_1, \dots, U_t\}$, for each $i = 1, \dots, t$, there exists $x^{(i)}\rho^{(i)}$ in H such that $1\rho^{(i)} = i$, and consequently $K_1^{x_1^{(i)}} = K_i$. Set $x := (x_1^{(1)}, x_1^{(2)} \dots, x_1^{(t)}) \in \mathrm{GL}(U)^t$. Then $H^{x^{-1}}$ induces the same transitive subgroup of S_t on the U_j, and, for $i = 1, \dots, t$, the subgroup of $\mathrm{GL}(U)$ induced by $(H^{x^{-1}})_i$ on the i^{th} tensor factor U_i is $x_1^{(i)} K_i (x_1^{(i)})^{-1} = K_1 = K$. Thus, replacing H by $H^{x^{-1}}$, we may assume that $K_1 = \cdots = K_t = K$. This means that $H \cap \mathrm{GL}(U)^t \leq K^t$. Finally consider a typical element $x\rho$ in the replaced subgroup H. For each i, we have shown that $K_i^{x_i} = K_{i\rho}$, that is, $x_i \in N_{\mathrm{GL}(U)}(K)$. □

Lemma 3.10. *Case* (iii) *above, with* $t \geq 3$, *does not hold.*

Proof. Suppose that (iii) holds, with $t \geq 3$. By Lemma 3.9, we may assume that $H \leq (N_{\mathrm{GL}(U)}(K) \circ \cdots \circ N_{\mathrm{GL}(U)}(K)).S_t$ and $H \cap (\mathrm{GL}(U) \circ \cdots \circ \mathrm{GL}(U)) \leq K \circ \cdots \circ K$, where $N_{\mathrm{GL}(U)}(K)$ is an irreducible subgroup of $\mathrm{GL}(U)$. Let $\{e_1, \dots, e_m\}$ be a basis for U. Then the set $\mathbb{B}$ of m^t vectors $e_{i_1} \otimes \cdots \otimes e_{i_t}$ (where each $i_j \leq m$) forms a basis for Ω. (Since we have identified each of the U_i with U, the order in these tensor expressions matters.)

Consider the vector $v = e_1 \otimes e_1 \otimes \cdots \otimes e_1 + e_1 \otimes e_2 \otimes \cdots \otimes e_2$. In this representation for v as a sum of two basic tensors, the two summands have equal first tensor entries, and all the other pairs of tensor entries are linearly independent. Suppose that there is another representation of v as

$$v = u_1 \otimes \cdots \otimes u_t + w_1 \otimes \cdots \otimes w_t$$

where the $u_j, w_j \in U_j$, and there exists an i such that $\{u_i, w_i\}$ is linearly dependent, but for each $j \neq i$, $\{u_j, w_j\}$ is linearly independent. We claim that $i = 1$. Suppose, for a contradiction, that this is not the case. Recall that $t \geq 3$. Without loss of generality, we may assume that $i = 2$, and that $u_2 = w_2$. For each j, let $u_j = \sum_l c_{jl} e_l$ and $w_j = \sum_l d_{jl} e_l$ (so $c_{2l} = d_{2l}$ for all l). Then

$$v = \sum_{(j_1, \dots, j_t)} \Big(\prod_{l=1}^{t} c_{l\, j_l} + \prod_{l=1}^{t} d_{l\, j_l} \Big) (e_{j_1} \otimes \cdots \otimes e_{j_t}).$$

Equating the coefficients of $e_1 \otimes e_1 \otimes \cdots \otimes e_1$ in the two expressions for v as linear combinations in the basis $\mathbb{B}$ gives

$$1 = \prod c_{l1} + \prod d_{l1} = c_{21} \Big(\prod_{l \neq 2} c_{l1} + \prod_{l \neq 2} d_{l1} \Big) = c_{21}\alpha,$$

say. Therefore both c_{21} and α are non-zero. Next, equating the coefficients of $e_1 \otimes e_2 \otimes e_1 \otimes \cdots \otimes e_1$ gives $0 = c_{22}\alpha$, whence $c_{22} = 0$. Then, equating the coefficients of $e_1 \otimes e_2 \otimes \cdots \otimes e_2$ gives

$$1 = c_{22}\Big(c_{11} \prod_{l \geq 3} c_{l2} + d_{11} \prod_{l \geq 3} d_{l2}\Big),$$

which contradicts the fact that $c_{22} = 0$. Thus in any such expression for v, the value of i is 1.

Let Δ denote the H-orbit containing v, and note that by assumption H is primitive on Δ. Each vector z in Δ can be expressed as $z = u_1 \otimes \cdots \otimes u_t + w_1 \otimes \cdots \otimes w_t$, where the $u_j, w_j \in U_j$, and there exists an i such that u_i and w_i are linearly dependent, but for each $j \neq i$, u_j and w_j are linearly independent. It follows from our computation above that the value of i is uniquely determined by z; and we write $i = i(z)$. For $i = 1, \ldots, t$, let $\Delta(i) = \{z \in \Delta \mid i(z) = i\}$. Then the subsets $\Delta(i)$ $(1 \leq i \leq t)$ form a system of imprimitivity for H in Δ, and since H is primitive on Δ, it follows that they have size 1. Thus $\Delta(1) = \{v\}$, and it follows that $H_v = H_1$. This means that $|\Delta| = t$. However, since H induces an irreducible linear group on Ω, Δ must contain a basis of Ω whence $|\Delta| \geq m^t > t$, which is a contradiction. □

Lemma 3.11. *Case* (iii) *above, with* $t = 2$*, does not hold.*

Proof. Suppose that (iii) holds, with $t = 2$, so by Lemma 3.9, we may assume that $H \leq (N_{\mathrm{GL}(U)}(K) \circ N_{\mathrm{GL}(U)}(K)).S_2$ and $H \cap (\mathrm{GL}(U) \circ \mathrm{GL}(U)) \leq K \circ K$, where $N_{\mathrm{GL}(U)}(K)$ is an irreducible subgroup of $\mathrm{GL}(U)$. Moreover, $L := H \cap (K \circ K)$ has index 2 in H. As in Lemma 3.9 we will work in the group $N_{\mathrm{GL}(U)}(K) \wr S_2$, acting unfaithfully on Ω. Let $\pi(x, x')$ and $\pi(y, y')$ be elements of $H \setminus L$, where $x, x', y, y' \in N_{\mathrm{GL}(U)}(K)$ and $\pi = (12) \in S_2$. Then L contains the elements

$$\pi(x, x')\pi(y, y') = (x'y, xy') \text{ and } \pi(x, x')(y^{-1}, y'^{-1})\pi = (x'y'^{-1}, xy^{-1}).$$

Hence $x \equiv y \equiv x'^{-1} \equiv y'^{-1} \pmod{K}$. Thus $H \leq N \wr S_2$, where $N = \langle K, x \rangle$, and H contains $\pi(x, x^{-1}k)$ for some $k \in K$.

Let $\{e_1, \ldots, e_m\}$ be a basis for U, so that the set $\mathbb{B}$ of m^2 vectors $e_i \otimes e_j$ (for $i, j \leq m$) forms a basis for Ω. Suppose first that $m = 2$, so $n = 4$, and since H is insoluble, $2^a \geq 4$. Since H is not realizable over a proper subfield, and H is insoluble, it follows (see [3, Section 260]) that H involves $\mathrm{SL}(2, 2^a)$. This implies that H has an element of order $2^a - 1$, contradicting Lemma 3.1.

Hence $m \geq 3$. Let $v = e_1 \otimes e_1 + e_2 \otimes e_2$, and let $\mathrm{stab}(W)$ denote the subgroup of $\mathrm{GL}(U)$ which leaves the subspace $W := \langle e_1, e_2 \rangle$ invariant (setwise). We claim that $H_v \leq \mathrm{stab}(W) \wr S_2$. Let $\pi(h, h') \in H_v$. Then $v = v(h, h') = (e_1 h) \otimes (e_1 h') + (e_2 h) \otimes (e_2 h')$. Set $e_i h = \sum_l c_{il} e_l$ and $e_i h' = \sum_l c'_{il} e_l$. Then $v =$

$\sum_{i,j}(c_{1i}c'_{1j}+c_{2i}c'_{2j})(e_i\otimes e_j)$, so

$$\begin{aligned} c_{11}c'_{11}+c_{21}c'_{21}&=1\\ c_{12}c'_{12}+c_{22}c'_{22}&=1, \quad \text{and}\\ c_{1i}c'_{1j}+c_{2i}c'_{2j}&=0, \quad \text{if } (i,j)\neq(1,1) \text{ or } (2,2). \end{aligned}$$

Define

$$A_{ij}=\begin{pmatrix} c_{1i} & c_{2i}\\ c_{1j} & c_{2j}\end{pmatrix} \quad \text{and} \quad A'_{ij}=\begin{pmatrix} c'_{1i} & c'_{2i}\\ c'_{1j} & c'_{2j}\end{pmatrix}.$$

The equations above imply that $A_{12}(A'_{12})^{\mathrm{tr}}=I$, and for $j\geq 3$,

$$A_{12}(A'_{1j})^{\mathrm{tr}}=\begin{pmatrix}1&0\\0&0\end{pmatrix}$$

and hence

$$(A'_{1j})^{\mathrm{tr}}=A_{12}^{-1}\begin{pmatrix}1&0\\0&0\end{pmatrix}=\begin{pmatrix}b&0\\c&0\end{pmatrix}$$

for some b,c. It follows that $c'_{1j}=c'_{2j}=0$ for all $j\geq 3$. Similarly, for $j\geq 3$,

$$A'_{12}A_{1j}^{\mathrm{tr}}=\begin{pmatrix}1&0\\0&0\end{pmatrix}$$

and hence

$$A_{1j}^{\mathrm{tr}}=(A'_{12})^{-1}\begin{pmatrix}1&0\\0&0\end{pmatrix}=\begin{pmatrix}b'&0\\c'&0\end{pmatrix}$$

for some b',c', so $c_{1j}=c_{2j}=0$ for all $j\geq 3$. Thus h,h' both leave $W=\langle e_1,e_2\rangle$ invariant, and so $H_v\leq \mathrm{stab}(W)\wr S_2$, proving our claim.

Since $m\geq 3$, $H\cap(\mathrm{stab}(W)\wr S_2)$ is a proper subgroup of H containing H_v, and since H_v is maximal in H it follows that $H_v=H\cap(\mathrm{stab}(W)\wr S_2)$. The same argument shows that $H_{v(u,u')}=H\cap(\mathrm{stab}(W)\wr S_2)$, where $v(u,u')=u\otimes u+u'\otimes u'$, for any basis u,u' of W. Suppose that H_v stabilises $\langle e_1\otimes e_1\rangle$. By maximality, H_v is equal to the stabilizer of $\langle e_1\otimes e_1\rangle$, and by Lemma 3.1, we have that H_v stabilises $e_1\otimes e_1$. The same argument proves that H_v stabilises $u\otimes u$ for each $u\in W$, and applying it again to any 2-dimensional subspace of U containing e_1 we have that H_v stabilises $u\otimes u$ for each $u\in U$. It follows that $H_v\cap(\mathrm{GL}(U)\circ\mathrm{GL}(U))$ is a subgroup of scalar matrices, and by Lemma 3.1 is trivial. Hence $|H_v|\leq 2$. Since H is primitive on the orbit v^H, it follows (see [30, 18.7]) that H is soluble, which is a contradiction. Thus H_v does not stabilise $\langle e_1\otimes e_1\rangle$.

If $a>1$ then, taking $b\in\mathrm{GF}(2^a)\setminus\{0,1\}$ and $u=e_1, u'=be_2$, we see that H_v stabilises $v'=e_1\otimes e_1+b^2\,e_2\otimes e_2$, and hence also stabilises $\langle e_1\otimes e_1\rangle$, which is a contradiction. Hence $\mathrm{GF}(2^a)=\mathrm{GF}(2)$. In this case the condition that H_v stabilise $v(u,u')$, for all bases u,u' for W, implies that the subgroup of $\mathrm{GL}(W)\wr S_2$ induced by H_v is contained in $\langle (h, h^{-1})\rangle \cdot \langle \pi \rangle \cong S_3$, where $\pi : u \otimes v \mapsto v \otimes u$ for all u, v, and where

$$h = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$$

with respect to the basis e_1, e_2 of W. This means also that the subgroup of $\mathrm{GL}(W) \wr S_2$ induced by $L \cap H_v$ is contained in $\langle (h, h^{-1})\rangle \cong Z_3$. Note that $h\colon e_1 \to e_2 \to e_1 + e_2$.

Recall that $H \leq N \wr S_2$, where $N = \langle K, x\rangle \leq N(K)$, and K is the subgroup of $\mathrm{GL}(U)$ induced by $H \cap (\mathrm{GL}(U) \times \mathrm{GL}(U))$. Also, H contains $\pi(x, x^{-1}k)$ for some $k \in K$. Suppose that the group N is intransitive on the nonzero vectors of U. Then we may assume that e_1, e_2 lie in different N-orbits. In this case the subgroup of $\mathrm{GL}(W) \wr S_2$ induced by H_v is contained in $\langle \pi \rangle$. In particular H_v stabilises $e_1 \otimes e_1$ which is not the case. Hence N is transitive on $U^{\#}$. By the definition of a, and since $a = 1$, we know that N is not contained in $\mathrm{GL}(m/a', 2^{a'}).a'$ for any divisor $a' > 1$ of m. Hence, by [17, Appendix], N is either $\mathrm{GL}(m, 2)$, or $\mathrm{Sp}(m, 2)$ (m even), or $N = \mathrm{G}_2(2)'$ or $\mathrm{G}_2(2)$ (with $m = 6$), or $N = A_7$ (with $m = 4$). We obtain a final contradiction by showing that in all cases there is a 2-dimensional subspace W of U for which the stabilizer of $W \otimes W$ in L induces at least an S_3 on $W \otimes W$, contradicting the fact that this stabilizer was shown to induce at most Z_3. This holds for any 2-subspace W if $N = \mathrm{GL}(m, 2)$, A_7, or $G_2(2)$, for any non-singular 2-subspace if $N = \mathrm{Sp}(m, 2)$, and for 315 of the 651 2-subspaces if $N = G_2(2)'$ (the information about $G_2(2)$ and $G_2(2)'$ was checked using GAP). □

4. Simply primitive affine groups

In this section we prove Theorem 1.3 and give further information (see Theorem 4.8) about the potential simply primitive, extremely primitive groups that may not have been listed in the statement of Theorem 1.3. *For the entire section, let $G \leq S_{2^d}$ be a simply primitive permutation group of affine type, of structure $G = Z_2^d.H$ with H almost simple. Let $\mathcal{M}$ denote the set of maximal subgroups of H, considered as matrix groups acting on $V = \mathrm{GF}(2)^d$. For $M \in \mathcal{M}$, let* $\mathrm{fix}(M)$ *denote the set of fixed vectors of M.*

One of our major tools is the following simple observation.

Lemma 4.1.

$$\sum_{M \in \mathcal{M}} (|\mathrm{fix}(M)| - 1) \leq 2^d - 1,$$

with equality if and only if G is extremely primitive. In particular, if $|\mathcal{M}| < 2^{d/2}$, then G is not extremely primitive.

Proof. For distinct $M_1, M_2 \in \mathcal{M}$, we have $\mathrm{fix}(M_1) \cap \mathrm{fix}(M_2) = \{0\}$ because there is no nontrivial fixed vector of $\langle M_1, M_2\rangle = H$. Hence each nonzero $v \in V$ occurs in at most one set fix(M) and $\sum_{M\in\mathcal{M}}(|\text{fix}(M)|-1) \le 2^d - 1$. Now G is extremely primitive if and only if each nonzero $v \in V$ indeed occurs in fix(M) for some $M \in \mathcal{M}$, that is, equality holds.

Now, for each $M \in \mathcal{M}$, $\dim(\text{fix}(M)) \le d/2$, since otherwise fix$(M)$ and fix(M^g) would have nontrivial intersection for $g \in H \setminus M$. Thus if $|\mathcal{M}| < 2^{d/2}$, then $\sum_{M\in\mathcal{M}}(|\text{fix}(M)|-1) < 2^d - 1$ and hence G is not extremely primitive by the previous paragraph. □

Lemma 4.2. *The groups $Z_2^d.H$ listed in the statement of Theorem* 1.3 *are extremely primitive.*

Proof. For the groups G in Theorem 1.3 (a) with $d \le 22$, and those in parts (b) and (c) with $d \le 12$, either we constructed G using the primitive group library of GAP, or we constructed H as a matrix group using the `atlasrep` package of GAP [31], and then computed the H-orbits in $V = \text{GF}(2)^d$ and the permutation actions of H on these orbits. We verified that each of these groups is extremely primitive. For the group $G = Z_2^{24}.Co_1$, generators of maximal subgroups M of type Co_2, $Z_2^{11}.M_{24}$, and Co_3 were constructed using `atlasrep`, enabling us to compute the dimensions of their fixed point spaces. Then we checked that the sum of $|\text{fix}(M)| - 1$ over the maximal subgroups M of H isomorphic to any of these three subgroups adds up to $2^{24} - 1$. Hence, by Lemma 4.1, this group G is also extremely primitive.

It is well known that the groups $H = \Omega^{\pm}(2k, 2)$ and $\Omega^{\pm}(2k, 2).2$, where $k \ge 7$, have two orbits on $\text{GF}(2)^{2k} \setminus \{0\}$ (the sets of singular and nonsingular vectors) and H acts primitively on each of these orbits.

What remains to prove is that the groups in Theorem 1.3 (b) with $d \ge 14$ are extremely primitive. In these cases $H = A_n$ or S_n with $n \in \{2k+1, 2k+2\}$, and H acts on $V = \text{GF}(2)^{2k}$ as on the deleted permutation module for its natural action of degree n. Let $U = \text{GF}(2)^n$ be the n-dimensional permutation module for the natural action of H, and let $W = \{(u_1, \ldots, u_n) \in U \mid \sum_{i=1}^n u_i = 0\}$. The stabilizer in H of a vector in U with ℓ nonzero coordinates is $H \cap (S_\ell \times S_{n-\ell})$, and two vectors of U are in the same H-orbit if and only if they have the same number of nonzero coordinates. Thus, H acts primitively on each of its orbits in U, apart from the orbit of vectors with $k+1$ nonzero entries when $n = 2k+2$. The subspace W is the union of those H-orbits that contain vectors with an even number of nonzero coordinates, so H acts primitively on each of its orbits in W except the orbit of vectors with $k+1$ nonzero entries in the case $n = 2k+2$, k odd. If $n = 2k+1$ then $V = W$ and so G is extremely primitive. If $n = 2k+2$ then V is the factor space of W, obtained by identifying the pairs of vectors $v_1 = (u_1, \ldots, u_n)$ and $v_2 = (1, 1, \ldots, 1) - (u_1, \ldots, u_n)$, for all $v_1 \in W$. Suppose without loss of generality that v_1 has ℓ nonzero entries and $\ell \le n/2$. Note that ℓ is even since $v_1 \in W$. If $\ell < n/2$ then the action of H on the orbit Δ of the pair $\{v_1, v_2\} \in V$ is permutationally isomorphic to the primitive action of H on the orbit of $v_1 \in W$, while if $\ell = n/2$ then v_1, v_2 correspond to disjoint

ℓ-sets, and so the H-action on Δ is permutationally isomorphic to its primitive action on partitions with two parts of size $n/2$. Hence in all cases H acts primitively on all of its orbits and G is extremely primitive. □

Now we start investigating the Lie-type simple groups of characteristic 2 that may occur as $\mathrm{Soc}(H)$ for an extremely primitive group G.

For a field F of characteristic 2 and an F-vectorspace V_0, the Frobenius automorphism $\sigma\colon x \mapsto x^2$ of F induces a semilinear map $\sigma\colon \sum_i \beta_i b_i \mapsto \sum_i \beta_i^2 b_i$ of V_0 with respect to a given F-basis $B = \{b_1, \dots, b_m\}$ of V_0. If V_0 is an FH-module and k is a positive integer, then by $V_0^{(k)}$ we mean the 'twisted' FH-module with underlying vector space V_0 such that for $h \in H, h\colon v \mapsto v\sigma^{-k}h\sigma^k$. For $h = (h_{ij}) \in \mathrm{GL}(m, F)$, where the matrix is relative to the basis B, the Frobenius automorphism σ satisfies $\sigma^{-1}h\sigma = (h_{ij}^\sigma)$ in $\Gamma\mathrm{L}(m, F)$, and we write $h^\sigma = (h_{ij}^\sigma)$. Thus if $h \in H$ acts on V_0 with matrix $(h_{ij}) \in \mathrm{GL}(m, F)$ relative to the basis B, then h acts on $V_0^{(k)}$ by $h\colon v \mapsto vh^{\sigma^k}$. Moreover, the tensor product $W = V_0 \otimes V_0^{(1)} \otimes \cdots \otimes V_0^{(e-1)}$ becomes an FH-module with action defined by $h\colon v_1 \otimes v_2 \otimes \cdots \otimes v_e \mapsto v_1 h \otimes v_2 h^\sigma \otimes \cdots \otimes v_e h^{\sigma^{e-1}}$. For each e-tuple $\boldsymbol{i} = (i_1, \dots, i_e)$, with $1 \le i_j \le m$ for each j, let

$$\tilde{b}_{\boldsymbol{i}} = b_{i_1} \otimes b_{i_2} \otimes \cdots \otimes b_{i_e}$$

so that the set $\mathbb{B}$ of all such $\tilde{b}_{\boldsymbol{i}}$ is an F-basis for W. If π denotes the element of $\mathrm{GL}(W)$ defined by $\tilde{b}_{\boldsymbol{i}}\pi = \tilde{b}_{\boldsymbol{i}^*}$, where $\boldsymbol{i}^* = (i_e, i_1, \dots, i_{e-1})$, then $\tilde{b}_{\boldsymbol{i}} h^\sigma = \tilde{b}_{\boldsymbol{i}} \pi h \pi^{-1}$, for each $\tilde{b}_{\boldsymbol{i}} \in \mathbb{B}$. Thus the element σ of $\Gamma\mathrm{L}(m, F)$ acts on W as π^{-1}, and we shall denote it still as σ.

Lemma 4.3. *Suppose that $G = Z_2^d.H$ is extremely primitive and simply primitive, that H is of Lie type defined over the field* $\mathrm{GF}(2^e)$ *with socle H_0, and let a be the largest integer such that $H \le \mathrm{GL}(d/a, 2^a).a$. Then the following hold.*

(i) *$a = 1$ and $d = m^e$ for some integer m;*

(ii) *there is an absolutely irreducible m-dimensional* $\mathrm{GF}(2^e)H_0$*-module V_0 with basis B such that $V \otimes \mathrm{GF}(2^e) = V_0 \otimes V_0^{(1)} \otimes \cdots \otimes V_0^{(e-1)}$ with basis $\mathbb{B}$ defined as above. Moreover, V can be identified with the* $\mathrm{GF}(2)$*-subspace $\widetilde{V}$ consisting of all vectors $\sum_{\boldsymbol{i}} \lambda_{\boldsymbol{i}} \tilde{b}_{\boldsymbol{i}}$ such that $\lambda_{\boldsymbol{i}^*} = \lambda_{\boldsymbol{i}}^2$ for all $\tilde{b}_{\boldsymbol{i}} \in \mathbb{B}$.*

Proof. First note that $2^e - 1$ divides $|H|$. Hence, if $\gcd(2^e - 1, 2^a - 1) > 1$ or, equivalently, $\gcd(e, a) > 1$ then H has an element of prime order $r \mid 2^a - 1$. This contradicts Lemma 3.1, and hence $\gcd(e, a) = 1$.

Let $H_0 := \mathrm{Soc}(H)$. By Lemma 3.6, H_0 is absolutely irreducible on V regarded as a $\mathrm{GF}(2^a)$-module $\mathrm{GF}(2^a)^{d/a}$ and H is not realisable over a proper subfield. Hence we are in the situation considered in [13, 5.4.6, 5.4.7]. If H_0 is untwisted or of type ${}^2B_2, {}^2G_2$, or ${}^2F_4$ then [13, 5.4.6(i), 5.4.7(b)] imply that $a|e$. Using $\gcd(a, e) = 1$, we obtain $a = 1$. If H_0 is of type ${}^2A_n$, ${}^2D_n$, or ${}^2E_6$ then [13, 5.4.6(ii)] implies that either $a \mid e$ whence $a = 1$, or $a \mid 2e$ but a does not divide e. In the latter case, $\gcd(a, e) = 1$ gives that $a = 2$. However, H_0 has elements of order 3, contradicting Lemma 3.1 so in this case also $a = 1$. Finally, if H_0 is of type ${}^3D_4$ then [13, 5.4.7(a)] implies that either $a \mid e$ whence $a = 1$, or $a \mid 3e$ but a does not divide e. In the latter case $a = 3$ and, since H_0 contains elements of order 7, Lemma 3.1 gives a contradiction. Hence in all cases $a = 1$.

Appealing again to [13, 5.4.6, 5.4.7], and to the proof of [16, Theorem 2.3] (referred to in [13, 5.4.7(b)]), we obtain that there is an absolutely irreducible FH_0-module M of dimension m over the algebraic closure F of GF(2^e), with basis $B = \{b_1, \dots, b_m\}$, such that $V \otimes F$ is isomorphic to the FH_0-module $W := M \otimes M^{(1)} \otimes \cdots \otimes M^{(e-1)}$ with basis $\mathbb{B}$, defined as above. In particular $d = m^e$, completing the proof of part (i). Moreover, $H \le \Gamma\mathrm{L}(W) = \Gamma\mathrm{L}(d, F)$.

Since $a = 1$, the GF(2)H-module V can be identified with a d-dimensional, H-invariant, GF(2)-subspace of W. Such a subspace must be fixed elementwise by σ (under the action described above), and hence must be contained in the subset $\widetilde{V}$ of all vectors of W fixed by σ. It is straightforward to compute that $\widetilde{V}$ consists of all $\sum_{\boldsymbol{i}} \lambda_{\boldsymbol{i}} \tilde{b}_{\boldsymbol{i}}$ such that $\lambda_{\boldsymbol{i}^*} = \lambda_{\boldsymbol{i}}^2$ for all $\boldsymbol{i}$. Clearly $\widetilde{V}$ is a GF(2)-subspace. Let $\sum_{\boldsymbol{i}} \lambda_{\boldsymbol{i}} \tilde{b}_{\boldsymbol{i}} \in \widetilde{V}$. For any $\boldsymbol{i}$, there is a smallest positive integer $e(\boldsymbol{i})$ such that $i_j = i_{j+e(\boldsymbol{i})}$ for all j (reading subscripts modulo e), and since $\lambda_{\boldsymbol{i}^*} = \lambda_{\boldsymbol{i}}^2$ for all $\boldsymbol{i}$, it follows that $\lambda_{\boldsymbol{i}}^{2^{e(\boldsymbol{i})}} = \lambda_{\boldsymbol{i}}$ so that $\lambda_{\boldsymbol{i}} \in \mathrm{GF}(2^{e(\boldsymbol{i})})$. Also, clearly $e(\boldsymbol{i})$ divides e, and hence $\lambda_{\boldsymbol{i}} \in \mathrm{GF}(2^e)$. Further, cyclically shifting the subscripts $\boldsymbol{i}$ defines an equivalence on the set of basis vectors $\mathbb{B}$, where $\tilde{b}_{\boldsymbol{i}}$ and $\tilde{b}_{\boldsymbol{i}'}$ are equivalent if $\boldsymbol{i}'$ can be obtained from $\boldsymbol{i}$ by repeated cyclic shifts, and there are $e(\boldsymbol{i})$ basis vectors in the equivalence class of $\tilde{b}_{\boldsymbol{i}}$. Moreover, since $\lambda_{\boldsymbol{i}^*} = \lambda_{\boldsymbol{i}}^2$, the coefficient $\lambda_{\boldsymbol{i}}$ (which can be chosen arbitrarily in GF($2^{e(\boldsymbol{i})}$)) uniquely determines the coefficients $\lambda_{\boldsymbol{i}'}$ for all other $\tilde{b}_{\boldsymbol{i}'}$ equivalent to $\tilde{b}_{\boldsymbol{i}}$. It follows that $|\widetilde{V}|$ is equal to the product of $2^{e(\boldsymbol{i})}$ over all equivalence classes, that is, $|\widetilde{V}| = 2^{m^e} = 2^d$ so $\widetilde{V}$ has GF(2)-dimension d. Since also V has GF(2)-dimension d, it follows that V can be identified with $\widetilde{V}$, and in particular that $\widetilde{V}$ is H-invariant.

Recall that σ acts trivially on $\widetilde{V}$. We now examine the action on $\widetilde{V}$ of an arbitrary $h \in H \cap \mathrm{GL}(m, F)$ with matrix (h_{ij}) relative to B. For each $\boldsymbol{i} = (i_1, \dots, i_e)$,

$$\begin{aligned} \tilde{b}_{\boldsymbol{i}} h &= b_{i_1} h \otimes b_{i_2} h^{\sigma} \otimes \cdots \otimes b_{i_e} h^{\sigma^{e-1}} \\ &= \otimes_{k=1}^{e} \Big(\sum_{j_k} (h_{i_k j_k} b_{j_k})^{\sigma^{k-1}} \Big) = \otimes_{k=1}^{e} \Big(\sum_{j_k} (h_{i_k j_k}^{2^{k-1}} b_{j_k}) \Big). \end{aligned}$$

Consider the tuples $\boldsymbol{i} = (i, i \dots, i)$ and $\boldsymbol{i}' = (j, j \dots, j)$, and note that $e(\boldsymbol{i}) = e(\boldsymbol{i}') = 1$. Then $\tilde{b}_{\boldsymbol{i}} \in \widetilde{V}$ and hence $\tilde{b}_{\boldsymbol{i}} h \in \widetilde{V}$. Thus the coefficient of $\tilde{b}_{\boldsymbol{i}'}$ in $\tilde{b}_{\boldsymbol{i}} h$, which by the above calculation is $\prod_{k=1}^{e} h_{ij}^{2^{k-1}} = h_{ij}^{2^e-1}$, should lie in $\mathrm{GF}(2^{e(\boldsymbol{i}')}) = \mathrm{GF}(2)$. Hence $h_{ij}^{2^e-1} = 0$ or 1, or equivalently, $h_{ij} \in \mathrm{GF}(2^e)$. Since this holds for all i, j, it follows that the matrix $(h_{ij}) \in \mathrm{GL}(m, 2^e)$. Thus GF($2^e$) is a splitting field for this representation of H and hence $\tilde{V}$ lies in the GF$(2^e)H$-invariant subspace $V_0 \otimes V_0^{(1)} \otimes \cdots \otimes V_0^{(e-1)}$, where V_0 is the restriction of M to GF(2^e). This completes the proof. □

Lemma 4.4. *Let $G, H, e, V_0, \mathbb{B}, \tilde{V}$ be as in Lemma* 4.3 *with G extremely primitive. Then either $e = m = 2$ and* $\mathrm{Soc}(H) = \mathrm{SL}(2,4)$ *as in Theorem* 1.3 (b)*, or $e = 1$.*

Proof. Suppose that $e \geq 2$. For $v \in \tilde{V}$ and $\tilde{b} \in \mathbb{B}$, let $c_v(\tilde{b})$ denote the coefficient of $\tilde{b}$ in the expression for v as a linear combination of the basis $\mathbb{B}$, that is, $v = \sum_{\tilde{b}\in\mathbb{B}} c_v(\tilde{b})\tilde{b}$.

For $1 \leq j \leq m$, let M_j denote the stabilizer in H of the vector $v_j := \tilde{b}_{(j,\ldots,j)} = b_j \otimes \cdots \otimes b_j \in \mathbb{B}$. Since G is extremely primitive, M_j is maximal in H, so $M_j = H_{\langle b_j \rangle}$ in the H-action on V_0. In particular the M_j are non-trivial, and hence are not all equal. Thus there are indices j_1, j_2 such that $M_{j_1} \neq M_{j_2}$. Without loss of generality, we may assume that $j_1 = 1$ and $j_2 = 2$.

Next, consider the stabilizer $M_{1,2}$ of $v := v_1 + v_2 \in \tilde{V}$. Since H is extremely primitive, $M_{1,2}$ is maximal in H, and therefore contains $M_1 \cap M_2$ as a proper subgroup. Suppose that $h \in \mathrm{GL}(m, 2^e)$ fixes v, and in the action of h on V_0 let

$$b_1 h = \sum_{j=1}^{m} \alpha_{1j} b_j, \quad b_2 h = \sum_{j=1}^{m} \alpha_{2j} b_j \tag{1}$$

with $\alpha_{i,j} \in \mathrm{GF}(2^e)$. Since $vh = v \in \tilde{V}$, we have $c_{vh}(\tilde{b}_{\boldsymbol{i}} *) = c_{vh}(\tilde{b}_{\boldsymbol{i}})^2$, for all $\boldsymbol{i}$, by Lemma 4.3. For each j,

$$c_{vh}(v_j) = \prod_{i=0}^{e-1} \alpha_{1j}^{2^i} + \prod_{i=0}^{e-1} \alpha_{2j}^{2^i} = \alpha_{1j}^{2^e-1} + \alpha_{2j}^{2^e-1}$$

and each summand lies in GF$(2) = \{0, 1\}$, so $c_{vh}(v_j) = 1$ if and only if exactly one of $\alpha_{1j}, \alpha_{2,j}$ is nonzero. In particular, exactly one of α_{11} and α_{21} is nonzero. If, for some $j \geq 3$, both $\alpha_{1j}, \alpha_{2,j}$ are nonzero, then

$$c_{vh}(\tilde{b}_{(1,j,\ldots,j)}) = \alpha_{11}\alpha_{1j}^{2+4+\cdots+2^{e-1}} + \alpha_{21}\alpha_{2j}^{2+4+\cdots+2^{e-1}}$$

is nonzero because exactly one of the summands is nonzero. This contradicts the fact that $vh = v$. Thus, for each $j \geq 3$, $\alpha_{1j} = \alpha_{2j} = 0$, and so either $b_1 h = \alpha_{11} b_1, b_2 h = \alpha_{22} b_2$, or $b_1 h = \alpha_{12} b_2, b_2 h = \alpha_{21} b_1$. Moreover each such element h fixes v. Elements h in H of the first type lie in the proper subgroup $M_1 \cap M_2$ of $M_{1,2}$, and hence, in its action on V_0, $M_{1,2}$ fixes $\langle b_1, b_2 \rangle$ and interchanges the 1-spaces $\langle b_1 \rangle$ and $\langle b_2 \rangle$. Since $M_j = H_{\langle b_j \rangle}$ for each j, it follows that $|M_{1,2} : M_1 \cap M_2| = 2$. If $m \geq 3$ then $M_{1,2}$ lies in the proper subgroup $H_{\langle b_1, b_2 \rangle}$, and the maximality of $M_{1,2}$

implies that $M_{1,2} = H_{\langle b_1, b_2 \rangle}$. On the other hand, if $m = 2$, we only know that $M_{1,2}$ is the setwise stabilizer of $\{\langle b_1 \rangle, \langle b_2 \rangle\}$ and maximal in H.

Next suppose that $e \geq 3$ and consider the stabilizers $M = M(\lambda)$ in H of the vectors of the form

$$u = u(\lambda) := \lambda \tilde{b}_{(1,2,\ldots,2)} + \lambda^2 \tilde{b}_{(2,1,2,\ldots,2)} + \cdots + \lambda^{2^{e-1}} \tilde{b}_{(2,\ldots,2,1)} \in \widetilde{V}$$

where $\lambda \in \mathrm{GF}(2^e)^\#$. Suppose that $h \in \mathrm{GL}(m, 2^e)$ such that h fixes u, and suppose that (1) holds. Since $uh = u$, for each j,

$$c_{uh}(v_j) = \sum_{i=0}^{e-1} \lambda^{2^i} \alpha_{1j}^{2^i} \alpha_{2j}^{2^e-1-2^i} = 0,$$

so if $\alpha_{2j} \neq 0$ then

$$\sum_{i=0}^{e-1} (\lambda \alpha_{1j} \alpha_{2j}^{-1})^{2^i} = 0. \tag{2}$$

Now

$$c_{uh}(\tilde{b}_{(1,2,\ldots,2)}) = \lambda \alpha_{11} \alpha_{22}^{2^e-2} + \alpha_{21} \sum_{i=1}^{e-1} \lambda^{2^i} \alpha_{12}^{2^i} \alpha_{22}^{2^e-2-2^i} = \lambda$$

and since each summand is a multiple of α_{22}, it follows that $\alpha_{22} \neq 0$. (This deduction requires $e \geq 3$.) Thus $\alpha_{22}^{2^e-1} = 1$, and using (2) we obtain

$$\alpha_{11}\alpha_{22}^{-1} + \alpha_{21}\alpha_{22}^{-1}(\alpha_{12}\alpha_{22}^{-1}) = 1, \text{ so } \alpha_{22}^2 = \alpha_{11}\alpha_{22} + \alpha_{21}\alpha_{12}. \tag{3}$$

Next,

$$c_{uh}(\tilde{b}_{(2,1,\ldots,1)}) = \lambda \alpha_{12} \alpha_{21}^{2^e-2} + \alpha_{22} \sum_{i=1}^{e-1} \lambda^{2^i} \alpha_{11}^{2^i} \alpha_{21}^{2^e-2-2^i} = 0.$$

Suppose that $\alpha_{21} \neq 0$. Then this equation becomes, using (2), $\alpha_{12} = \alpha_{22}\alpha_{11}\alpha_{21}^{-1}$. Substituting in (3) yields $\alpha_{22} = 0$, which is a contradiction. Thus $\alpha_{21} = 0$, and (3) implies $\alpha_{11} = \alpha_{22}$. Using these values we find, for $j \geq 3$,

$$c_{uh}(\tilde{b}_{(1,j,2,\ldots,2)}) = \lambda \alpha_{11} \alpha_{2j}^2 \alpha_{22}^{2^e-4} = 0$$

which implies $\alpha_{2j} = 0$ for all $j \geq 3$. Then we have also

$$c_{uh}(\tilde{b}_{(j,2,\ldots,2)}) = \lambda \alpha_{1j} \alpha_{22}^{2^e-2} = 0$$

which implies that $\alpha_{1j} = 0$ for all $j \geq 3$. Thus h fixes $\langle b_1, b_2 \rangle$ setwise. If $m \geq 3$, then this implies that $M \leq M_{1,2} = H_{\langle b_1, b_2 \rangle}$, and by the maximality of M, equality holds. This in turn implies that some element of M interchanges $\langle b_1 \rangle$ and $\langle b_2 \rangle$, but we have just proved that this is not the case. Thus $m = 2$. Now the fact that $\alpha_{21} = 0$ implies that h fixes $\langle b_2 \rangle$. Hence $M \le M_2 = H_{\langle b_2 \rangle}$ and maximality implies that $M = M_2$. In fact $M_2 = M(\lambda)$ for each $\lambda \in \mathrm{GF}(2^e)^\#$. Since $M_2 \neq M_1$, some element of M_2 moves $\langle b_1 \rangle$, and we may assume that h is such an element. Thus $\alpha_{12} \neq 0$, and (2) with $j = 2$ implies that

$$\sum_{i=0}^{e-1} (\lambda\alpha)^{2^i} = 0 \quad \text{where } \alpha = \alpha_{21}\alpha_{22}^{-1}$$

that is to say, $\lambda\alpha$ has trace 0 in $\mathrm{GF}(2^e)$ (over $\mathrm{GF}(2)$). Since $\alpha \neq 0$, and this holds for all $\lambda \neq 0$, it follows that all nonzero elements of $\mathrm{GF}(2^e)$ have trace zero, which is a contradiction. Thus we have proved that $e = 2$.

If $e = m = 2$, then $\mathrm{Soc}(H) = \mathrm{SL}(2,4) < \mathrm{GL}(4,2)$ and we have the unique degree 4 absolutely irreducible representation of this group, that is, Theorem 1.3 (b) holds. Assume then that $m \ge 3$, so $M_{1,2} = H_{\langle b_1, b_2 \rangle}$ and elements of this subgroup fix or interchange $\langle b_1 \rangle$ and $\langle b_2 \rangle$. To complete the proof we consider the vectors $w = w(\lambda) := \lambda\tilde{b}_{(1,2)} + \lambda^2\tilde{b}_{(2,1)}$, where $\lambda \in \mathrm{GF}(4)^\#$. Note that $\lambda^3 = 1$. It follows from Lemma 4.3 that $w \in \widetilde{V}$. Suppose that $h \in \mathrm{GL}(V_0) = \mathrm{GL}(m,4)$ such that h fixes w and suppose that (1) holds. Then, for each j,

$$c_{wh}(v_j) = \lambda\alpha_{1j}\alpha_{2j}^2 + \lambda^2\alpha_{2j}\alpha_{1j}^2 = 0, \text{ so } \alpha_{1j}\alpha_{2j}^2 = \lambda\alpha_{2j}\alpha_{1j}^2. \tag{4}$$

Next we compute, where $j \ge 3$,

$$\begin{aligned}
c_{wh}(\tilde{b}_{(1,2)}) = \lambda &\implies \lambda\alpha_{11}\alpha_{22}^2 + \lambda^2\alpha_{21}\alpha_{12}^2 = \lambda,\\
c_{wh}(\tilde{b}_{(2,1)}) = \lambda^2 &\implies \lambda\alpha_{12}\alpha_{21}^2 + \lambda^2\alpha_{22}\alpha_{11}^2 = \lambda^2,\\
c_{wh}(\tilde{b}_{(j,1)}) = 0 &\implies \alpha_{1j}\alpha_{21}^2 = \lambda\alpha_{2j}\alpha_{11}^2,\\
c_{wh}(\tilde{b}_{(j,2)}) = 0 &\implies \alpha_{1j}\alpha_{22}^2 = \lambda\alpha_{2j}\alpha_{12}^2.
\end{aligned}$$

Suppose first that $\alpha_{22} = 0$. Then the second equation above implies that $\alpha_{12}\alpha_{21}^2 = \lambda \neq 0$. The fourth equation gives $\alpha_{2j} = 0$, and then the third gives $\alpha_{1j} = 0$, for all $j \ge 3$. Thus $h \in M_{1,2}$ and h does not fix $\langle b_2 \rangle$. It follows that h interchanges $\langle b_1 \rangle$ and $\langle b_2 \rangle$, and hence $\alpha_{11} = 0$, and the matrix h induces on $\langle b_1, b_2 \rangle$ (relative to the basis $\{b_1, b_2\}$) is

$$\begin{pmatrix} 0 & \lambda\alpha_{21} \\ \alpha_{21} & 0 \end{pmatrix}.$$

Similarly if $\alpha_{11} = 0$ then h fixes $\langle b_1, b_2 \rangle$ setwise and induces this matrix on it. Suppose then that both α_{11} and α_{22} are non-zero. If both of α_{12}, α_{21} are non-zero, then (4) implies that $\alpha_{22} = \lambda\alpha_{12}$ and $\alpha_{21} = \lambda\alpha_{11}$, and substituting in the first equation yields $\lambda = 0$, a contradiction. Thus one of α_{12}, α_{21} is zero. Without loss of generality suppose that $\alpha_{12} = 0$. Evaluating the fourth, and then the third of the equations above we find that $\alpha_{1j} = \alpha_{2j} = 0$ for all $j \geq 3$. Thus again $h \in M_{1,2}$. It follows that $M \leq M_{1,2}$, and maximality of M implies that $M = M(\lambda) = M_{1,2}$ for all λ. Let $h \in M_{1,2} \setminus (M_1 \cap M_2)$ so that h interchanges $\langle b_1 \rangle$ and $\langle b_2 \rangle$. Then we have that $\alpha_{12} = \lambda\alpha_{21} \neq 0$, and this must hold for all $\lambda \in \mathrm{GF}(4)^{\#}$. This is impossible, and thus the proof is complete. □

Thus to complete the analysis of the case where $H_0 = \mathrm{Soc}(H)$ is of Lie type in characteristic 2, we must deal with such groups H defined over GF(2) and acting absolutely irreducibly on a GF(2)H-module $V = V_0$, with V_0 as in Lemma 4.3. It follows from the proof of [13, Proposition 5.4.6] and [13, Remark 5.4.7 (a)], that for every case apart from $H_0 = {}^2F_4(2)'$, the module V_0 is one of the so-called 2-restricted highest weight modules – the 'basic building blocks' for absolutely irreducible modules for these groups, see [9]. In the exceptional case where $H_0 = {}^2F_4(2)'$, there are exactly two non-trivial absolutely irreducible representations of H that are realisable over GF(2), and these have degrees 26 and 246, see [12, p.188]. We do not need any details of the theory of even characteristic representations; we only use the list of small-dimensional representations and their weights given in [21].

Next we examine, for classical groups, some small-dimensional modules defined over GF(2): the alternating square (in Lemma 4.5) and the adjoint (in Lemma 4.6) of the natural module. The H-actions on these modules are explained carefully in the proofs.

Lemma 4.5. *If H is a classical group defined over* GF(2) *and V is the alternating square module for H, then G is extremely primitive if and only if d,* Soc(H) *occur in one of the columns of Table* 1. *These examples occur in Theorems* 1.2 (b) *or* 1.3 (b) ,(c).

Table 1. Table for Lemma 4.5.

d	6	4	4	6
$\mathrm{Soc}(H)$	$\mathrm{SL}(4,2)$	$\mathrm{Sp}(4,2)'$	$\Omega^-(4,2)$	$\mathrm{PSU}(4,2)$
$\cong$	A_8	A_6	A_5	$\Omega^-(6,2)$

Proof. Case 1: $\mathrm{Soc}(H) = \mathrm{SL}(n,2)$ *for some* $n \geq 4$. Let $B = \{b_1, \ldots, b_n\}$ be a basis for the natural module W of $\mathrm{Soc}(H)$. A basis of the alternating square module $W^{\wedge 2}$ is the set $B^{\wedge 2} := \{b_i \wedge b_j \mid 1 \leq i < j \leq n\}$. If some $h \in \mathrm{Soc}(H)$ has matrix $h = (\alpha_{ij})$ relative to B then the action of h on $B^{\wedge 2}$ is defined by

$$b_i \wedge b_j \mapsto \sum_{k<l} (\alpha_{i,k}\alpha_{j,l} + \alpha_{i,l}\alpha_{j,k})\ b_k \wedge b_l. \tag{5}$$

If $n = 4$ then the actions of $\mathrm{SL}(4,2) \cong A_8$ and $\mathrm{SL}(4,2).2 \cong S_8$ on the alternating square module are isomorphic to their actions on the deleted permutation module and we get extremely primitive examples (see Lemma 4.2). Suppose now that $n > 4$. In this case $\mathrm{SL}(n,2).2$ does not act on $W^{\wedge 2}$ and so $H = \mathrm{Soc}(H)$. We prove that the stabilizer $M_{14,23}$ of $b_1 \wedge b_4 + b_2 \wedge b_3$ is not maximal in H, and hence that G is not extremely primitive.

Let $h \in M_{14,23}$ with $h = (\alpha_{ij})$ relative to B. We examine the entries α_{ik} for $5 \le k \le n$ and $1 \le i \le 4$. For some fixed $k \ge 5$, let $X_k := \{i \le 4 \mid \alpha_{ik} \ne 0\}$ and $\overline{X}_k := \{5-i \mid i \in X_k\}$. For any $\ell \ne k$, the coefficient of $b_k \wedge b_\ell$ in $(b_1 \wedge b_4 + b_2 \wedge b_3)h$ is 0; hence, by (5),

$$0 = \sum_{j=1}^{4} \alpha_{5-j,k}\alpha_{j\ell} = \sum_{j \in \overline{X}_k} \alpha_{5-j,k}\alpha_{j\ell} = \sum_{j \in \overline{X}_k} \alpha_{j\ell}. \tag{6}$$

Note that, if $j \in \overline{X}_k$, then either (i) $j \notin X_k$ so that $\alpha_{jk} = 0$, or (ii) $j \in X_k$ so that both $j, 5-j \in \overline{X}_k$ and $\alpha_{jk} + \alpha_{5-j,k} = 1 + 1 = 0$. Hence $\sum_{j \in \overline{X}_k} \alpha_{jk} = 0$ as well. Thus, the rows of h with indices in $\overline{X}_k$ sum to the zero vector. If $\overline{X}_k \ne \emptyset$ this gives a contradiction, so $\overline{X}_k = \emptyset$ and hence $X_k = \emptyset$ also. Thus $\alpha_{ik} = 0$ for all $i \le 4$ and $k \ge 5$, and hence $M_{14,23}$ fixes the subspace $U := \langle b_1, b_2, b_3, b_4 \rangle$ in its action on W. The subgroup of $\mathrm{GL}(U)$ induced by $M_{14,23}$ is isomorphic to $\mathrm{Sp}(4,2)$ because stabilising $b_1 \wedge b_4 + b_2 \wedge b_3$ in the alternating square of $\mathrm{SL}(4,2)$ is equivalent to stabilising a nondegenerate alternating form on U. Hence $M_{14,23}$ is a proper subgroup of the stabilizer of U and so is not maximal in H.

Case 2: $\mathrm{Soc}(H) = \mathrm{Sp}(n,2)'$ *with* $n \ge 4$*,* n *even.* If $n = 4$ then the actions of $\mathrm{Sp}(4,2)' \cong A_6$ and $\mathrm{Sp}(4,2) \cong S_6$ on the alternating square are isomorphic to their actions on the deleted permutation module and we get extremely primitive examples. Suppose that $n > 4$. In this case $H = \mathrm{Sp}(n,2)$. We consider H as a subgroup of $\mathrm{SL}(n,2)$ acting on W and $W^{\wedge 2}$ as defined in Case 1. We choose the basis B so that $\{b_{2i-1}, b_{2i}\}$ is a hyperbolic pair for $1 \le i \le n/2$. This means that H consists of those elements $h = (\alpha_{ij}) \in \mathrm{SL}(n,2)$ that for $1 \le i < j \le n$ satisfy

$$\sum_{k=1}^{n/2} \alpha_{i,2k-1}\alpha_{j,2k} + \alpha_{i,2k}\alpha_{j,2k-1} = \begin{cases} 1 & \text{if } \{b_i, b_j\} \text{ is a hyperbolic pair} \\ 0 & \text{otherwise} \end{cases} \tag{7}$$

and, since the invariant bilinear form J of $\mathrm{Sp}(n,2)$ satisfies $J = (J^{-1})^{\mathrm{tr}} = J^{-1}$, we also have $(\alpha_{ij})^{\mathrm{tr}} \in \mathrm{Sp}(n,2)$ and so

$$\sum_{k=1}^{n/2} \alpha_{2k-1,i}\alpha_{2k,j} + \alpha_{2k,i}\alpha_{2k-1,j} = \begin{cases} 1 & \text{if } \{\, b_i, b_j \,\} \text{ is a hyperbolic pair} \\ 0 & \text{otherwise.} \end{cases} \tag{8}$$

However, $H = \mathrm{Sp}(n,2)$ does not act on $W^{\wedge 2}$ irreducibly. For $w = \sum_{k,\ell} \lambda_{k\ell} b_k \wedge b_\ell \in W^{\wedge 2}$, let $\Lambda(w) := \sum_{k=1}^{n/2} \lambda_{2k-1,2k}$. Then $\widetilde{W} := \{w \in W^{\wedge 2} \mid \Lambda(w) = 0\}$ is a codimension 1 subspace. (Note that $\widetilde{W}$ consists of all $\sum_{k,\ell} \lambda_{k\ell} b_k \wedge b_\ell$ such that an even number of the coefficients $\lambda_{2i-1,2i}$ is non-zero.) This subspace is H-invariant, because for any $h = (\alpha_{ij}) \in H$ and $b_i \wedge b_j \in B^{\wedge 2}$, using (5) and (7), we see that $\Lambda((b_i \wedge b_j)h)$ is equal to

$$\sum_{k=1}^{n/2} \alpha_{i,2k-1}\alpha_{j,2k} + \alpha_{i,2k}\alpha_{j,2k-1} = \begin{cases} 1 & \text{if } \{b_i, b_j\} \text{ is a hyperbolic pair} \\ 0 & \text{otherwise.} \end{cases}$$

Also the subspace $\langle u \rangle$, where $u := \sum_{k=1}^{n/2} b_{2k-1} \wedge b_{2k}$, is H-invariant because for any $h = (\alpha_{ij}) \in H$ and $b_i \wedge b_j \in B^{\wedge 2}$, the coefficient of $b_i \wedge b_j$ in uh is

$$\sum_{k=1}^{n/2} \alpha_{2k-1,i}\alpha_{2k,j} + \alpha_{2k,i}\alpha_{2k-1,j} = \begin{cases} 1 & \text{if } \{b_i, b_j\} \text{ is a hyperbolic pair} \\ 0 & \text{otherwise} \end{cases}$$

by (8). If $n/2$ is odd then $\widetilde{W}$ is irreducible, $W^{\wedge 2} = \widetilde{W} \oplus \langle u \rangle$, and $\widetilde{W}$ is the alternating square module V. If $n/2$ is even, then $u \in \widetilde{W}$, the factor module $\widetilde{W}/\langle u \rangle$ is irreducible, and it is the alternating square module V. Let $w := b_1 \wedge b_4 + b_2 \wedge b_3 \in \widetilde{W}$, and let $v = w$ if $n/2$ is odd and $v = w + \langle u \rangle$ if $n/2$ is even. So $v \in V$. We shall prove that the stabilizer $M_{14,23}$ of v is not maximal in H and so G is not extremely primitive.

If $n/2$ is odd then $M_{14,23}$ consists of those $h \in H$ that stabilise w. If $n/2$ is even then $M_{14,23}$ is the union of those $h \in H$ that stabilise w and those $h \in H$ that map w to $w + u$. In either case those $h \in H$ that stabilise w were shown in Case 1 to stabilise $U = \langle b_1, b_2, b_3, b_4 \rangle \leq W$.

We claim that, if $n/2$ is even, then there is no $h \in H$ which maps w to $w + u$. Suppose, on the contrary, that there is an $h = (\alpha_{ij}) \in H$ such that $wh = w + u$. Let $k \geq 5$ be fixed and let $k' \in \{k-1, k+1\}$ be such that $\{b_k, b_{k'}\}$ is a hyperbolic pair. We define X_k and $\overline{X}_k$ as Case 1. Now $X_k \neq \emptyset$ as otherwise the coefficient of $b_k \wedge b_{k'}$ would be 0 in wh by (5). Also,(6) holds for all $\ell \notin \{k, k'\}$ because the coefficient of $b_k \wedge b_l$ is 0 in $w + u$.

We consider the possibilities for X_k. If $|X_k| = 1$, by symmetry say $X_k = \{1\}$, then by the definition of X_k, $\alpha_{3k} = \alpha_{4k} = 0$ and, by (6), $\alpha_{4,\ell} = 0$ for all $\ell \neq k'$. This gives a contradiction to (7) applied with $i = 3$ and $j = 4$. Hence $|X_k| \geq 2$ for all $k \geq 5$. Suppose next that $|X_k| = 4$. Then since the coefficient of $b_k \wedge b_{k'}$ in $w+u$ is 1 and in wh is $\sum_{i=1}^{4} \alpha_{ik'}$, $|X_{k'}|$ must be odd. Since $|X_{k'}| \geq 2$, we must have $|X_{k'}| = 3$ and by symmetry we may assume $X_{k'} = \{1, 2, 3\}$. Applying (6) with k and k', we obtain that for all $\ell \notin \{k, k'\}$ the sums $\sum_{j=1}^{4} \alpha_{j\ell} = 0$ and $\sum_{j=2}^{4} \alpha_{j\ell} = 0$. Hence $\alpha_{1,\ell} = 0$. This, combined with the fact $\alpha_{1,k} = \alpha_{2,k} = \alpha_{1,k'} = \alpha_{2,k'} = 1$, yields a contradiction by (7) applied with $i = 1$ and $j = 2$. Hence $2 \leq |X_k| \leq 3$ for all $k \geq 5$.

Suppose next that $|X_k| = 3$. By symmetry we may assume $X_k = \{1, 2, 3\}$. Then the coefficient of $b_k \wedge b_{k'}$ in $w + u$ is 1 and in wh is $\alpha_{2k'} + \alpha_{3k'} + \alpha_{4k'}$, and hence

$|X_{k'} \cap \{2,3,4\}|$ is odd. Suppose first that $|X_{k'}| = 3$. Then $|X_{k'} \cap \{2,3,4\}| \geq 2$ and so $X_{k'} = \{2,3,4\}$. Applying (6) with k and k', we obtain that for all $\ell \notin \{k,k'\}$ the sums $\sum_{j=2}^{4} \alpha_{j\ell} = 0$ and $\sum_{j=1}^{3} \alpha_{j\ell} = 0$. Adding these two equations, we obtain $\alpha_{1\ell} + \alpha_{4\ell} = 0$, that is, $\alpha_{1\ell} = \alpha_{4\ell}$. Now (7) yields a contradiction for $i = 1$ and $j = 4$. Thus, by the previous paragraph, we must have $|X_{k'}| = 2$, and hence $|X_{k'} \cap \{2,3,4\}| = 1$ (as it is odd). If $X_{k'} = \{1,4\}$ then applying (6) with k', we obtain $\alpha_{1\ell} = \alpha_{4\ell}$ for all $\ell \notin \{k,k'\}$ and then (7) yields a contradiction for $i = 1$ and $j = 4$. If $X_{k'} = \{1,2\}$ then applying (6) with k' we obtain $\alpha_{3\ell} = \alpha_{4\ell}$ for all $\ell \notin \{k,k'\}$ and then (7) yields a contradiction for $i = 3$ and $j = 4$. Finally if $X_{k'} = \{1,3\}$ then applying (6) with k and k' we obtain that, for all $\ell \notin \{k,k'\}$, the sum $\sum_{j=2}^{4} \alpha_{j\ell} = 0$ and $\alpha_{2\ell} = \alpha_{4\ell}$. Hence $\alpha_{3\ell} = 0$ and (7) yields a contradiction for $i = 3$ and $j = 4$.

Thus the only possibility remaining is that $|X_k| = 2$ for all $k \geq 5$. Let $\bar{X}_k = \{i,j\}$ and set $\{s,t\} := \{1,2,3,4\} \setminus \bar{X}_k$. In this case we also fix an $m \geq 5$, with $m \notin \{k,k'\}$ (since $n/2 > 2$ and $n/2$ is even, such an m exists). Applying (6) with k, we obtain that $\alpha_{im} = \alpha_{jm}$, and then also $\alpha_{sm} = \alpha_{tm}$ because $|X_m| = 2$. Applying (6) with k', we obtain that $\alpha_{pm} = \alpha_{rm}$ for $p,r \in \bar{X}_{k'}$. This pair $\{p,r\}$ is different from $\{i,j\}$ and $\{s,t\}$ because otherwise the coefficient of $b_k \wedge b_{k'}$ would be 0 in v. Hence all of the first four entries in column m of H are equal, contradicting $|X_m| = 2$. Thus there are no possibilities for X_k.

Summarizing, we have shown that the stabilizer $M_{14,23}$ of v fixes the subspace $U = \langle b_1, b_2, b_3, b_4 \rangle \leq W$. The group induced by $M_{14,23}$ on U is the intersection of two symplectic groups $\mathrm{Sp}(4,2)$ (one is the stabilizer of U in H, the other one is the stabilizer of $w \in W^{\wedge 2}$ in $\mathrm{SL}(n,2)$ acting on W). Computation in *GAP* shows that the group induced by $M_{14,23}$ on U is isomorphic to $S_4 \times Z_2$. Hence $M_{14,23}$ is a proper subgroup of the stabilizer of U in H and so is not maximal in H.

Case 3: $\mathrm{Soc}(H) = \Omega^{\pm}(n,2)$ *with n even, $n \geq 4$.* For $n = 4$, since H is almost simple, $\mathrm{Soc}(H) = \Omega^{-}(4,2) \cong \mathrm{SL}(2,4) \cong A_5$. The action of H on the alternating square module is isomorphic to the deleted permutation module action of A_5 or S_5, and hence G is extremely primitive. Suppose now that $n \geq 6$. In this case, H is a subgroup of $\mathrm{Sp}(n,2)$, and in its action on W we can choose the basis B such that the group induced by H on the subspace U above is $\mathrm{SO}^{+}(4,2)$. The alternating square module V for H is $\widetilde{W}$ if $n/2$ is odd and $\widetilde{W}/\langle u \rangle$ if $n/2$ is even. Again, we consider the stabilizer $M_{14,23}$ of v. Since $H \leq \mathrm{Sp}(n,2)$, we know that $M_{14,23} = H_w$ and fixes $U \leq W$. The group induced by $M_{14,23}$ on U is the intersection of an orthogonal group of plus type and a symplectic group; computation in *GAP* shows that it is isomorphic to $\mathrm{SL}(2,2)$. Hence $M_{14,23}$ is a proper subgroup of the stabilizer of U in H and so is not maximal in H.

Case 4: $\mathrm{Soc}(H) = \mathrm{PSU}(n,2)$ *with $n \geq 4$.* If $n = 4$ then the alternating square module of $\mathrm{PSU}(4,2) \cong \Omega^{-}(6,2)$ is isomorphic to the natural module of $\Omega^{-}(6,2)$, yielding two extremely primitive examples. For $n > 4$, the alternating square module of $\mathrm{PSU}(n,2)$ is not defined over GF(2). (It is defined over GF(4) and not GF(2) because its 2-restricted highest weight is ω_2 which is not invariant under the graph automorphism of the Dynkin diagram.) Thus by Lemma 4.4, and the discussion following it, G is not extremely primitive. □

Lemma 4.6. *Let* $\mathrm{Soc}(H) = \mathrm{SL}(n,2)$ *or* $\mathrm{PSU}(n,2)$ *and let* V *be the adjoint module of* H. *Then* G *is not extremely primitive.*

Proof. Case 1: $\mathrm{Soc}(H) = \mathrm{SL}(n,2)$ *with* $n \geq 3$. Suppose that $B = \{b_1, \ldots, b_n\}$ is a basis for the natural module W of $\mathrm{SL}(n,2)$ and let W^* be the dual of W with basis $B^* = \{b_1^*, \ldots, b_n^*\}$. For $h \in \mathrm{Soc}(H)$, if the matrix for h on W, written relative to the basis B, is $h = (\alpha_{ij})$ then the matrix of h on W^*, written relative to B^*, is (α_{ij}^*), where (α_{ij}^*) is the inverse transpose of (α_{ij}). The connection between (α_{ij}) and (α_{ij}^*) is given by

$$\sum_{k=1}^{n} \alpha_{i,k}\alpha_{j,k}^* = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{if } i \neq j \end{cases} \tag{9}$$

and

$$\sum_{k=1}^{n} \alpha_{k,i}\alpha_{k,j}^* = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{if } i \neq j. \end{cases} \tag{10}$$

We consider the n^2-dimensional vector space $W \otimes W^*$, with basis $B \otimes B^* := \{b_i \otimes b_j^* \mid 1 \leq i, j \leq n\}$. For $h \in H$ with matrix (α_{ij}) relative to B, the action of h on $W \otimes W^*$ is defined by

$$b_i \otimes b_j^* \mapsto \sum_{k,\ell} \alpha_{i,k}\alpha_{j,\ell}^* \; b_k \otimes b_\ell^*. \tag{11}$$

If $H = \mathrm{SL}(n,2).2$ and $\tau \in H$ conjugates all $h = (\alpha_{ij}) \in \mathrm{Soc}(H)$ to $h^\tau = (\alpha_{ij}^*)$ then τ acts on $B \otimes B^*$, and hence on $W \otimes W^*$ by

$$b_i \otimes b_j^* \mapsto b_j \otimes b_i^*. \tag{12}$$

The group H does not act on $W \otimes W^*$ irreducibly. For $w = \sum_{k,\ell} \lambda_{k\ell} b_k \otimes b_\ell^* \in W \otimes W^*$, let $\Lambda(w) := \sum_{k=1}^{n} \lambda_{k,k}$. Then $\widetilde{W} := \{w \in W \otimes W^* \mid \Lambda(w) = 0\}$ is a codimension 1 subspace. This subspace is H-invariant, because $\Lambda(w\tau) = \Lambda(w)$ for any w, and for any $h = (\alpha_{ij}) \in \mathrm{Soc}(H)$, $\Lambda(wh) = \sum_{i,j} \lambda_{ij} \Lambda((b_i \otimes b_j)h)$, and by (11) and (9),

$$\Lambda((b_i \otimes b_j^*)h) = \sum_{k=1}^{n} \alpha_{i,k}\alpha_{j,k}^* = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{if } i \neq j. \end{cases}$$

Let $u := \sum_{k=1}^{n} b_k \otimes b_k^*$. Then $\langle u \rangle$ is H-invariant because $u\tau = u$ and, for any $h = (\alpha_{ij}) \in \mathrm{Soc}(H)$ and $b_i \otimes b_j^* \in B \otimes B^*$, the coefficient of $b_i \otimes b_j^*$ in uh is

$$\sum_{k=1}^{n} \alpha_{k,i}\alpha_{k,j}^* = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{if } i \neq j \end{cases}$$

by (10). If n is odd then $\widetilde{W}$ is irreducible, $W \otimes W^* = \widetilde{W} \oplus \langle u \rangle$, and $\widetilde{W}$ is the adjoint module V. If n is even then $u \in \widetilde{W}$ and the factor module $\widetilde{W}/\langle u \rangle$ is irreducible, called the adjoint module V. Let $w := b_1 \otimes b_2^* + b_2 \otimes b_1^* \in \widetilde{W}$ and let $v = w$ if n is odd, and $v = w + \langle u \rangle$ if n is even, so in both cases $v \in V$. We shall prove that in either case the stabilizer $M_{12,21}$ of v is not maximal in H and so G is not extremely primitive.

If n is odd then $M_{12,21}$ consists of those $h \in H$ that stabilise w. If n is even then $M_{12,21}$ is the union of those $h \in H$ that stabilise w and those that map w to $w + u$. Since by (12), $w\tau = w$, we only need to consider elements of $\mathrm{Soc}(H)_v$. Suppose first that $h = (\alpha_{ij}) \in \mathrm{Soc}(H)$ stabilises w. For $k \geq 3$, let $X_k := \{i \leq 2 \mid \alpha_{ik} \neq 0\}$ and $\bar{X}_k := \{3 - i \mid i \in X_k\}$. Similarly, let $X_k^* := \{i \leq 2 \mid \alpha_{ik}^* \neq 0\}$ and $\bar{X}_k^* := \{3 - i \mid i \in X_k^*\}$. For any $\ell \leq n$, the coefficient of $b_k \otimes b_\ell^*$ in wh is 0. Hence, by (11), $\sum_{j \in \bar{X}_k} \alpha_{3-j,k}\alpha_{j\ell}^* = 0$. Thus if $X_k \neq \emptyset$ then a nontrivial linear combination of the rows of (α_{ij}^*) is the zero vector, which is a contradiction. Similarly, for any $\ell \leq n$ the coefficient of $b_\ell \otimes b_k^*$ in wh is 0. Hence $\sum_{j \in \bar{X}_k^*} \alpha_{3-j,\ell}\alpha_{jk}^* = 0$, and if $X_k^* \neq \emptyset$ then a nontrivial linear combination of the rows of h is the zero vector, which is a contradiction. Hence $\alpha_{ik} = \alpha_{ik}^* = 0$, for $1 \leq i \leq 2$, $3 \leq k \leq m$. Since $(\alpha_{ij}^*) = (h^{-1})^{\mathrm{tr}}$, this implies that also $\alpha_{ki} = 0$, for $1 \leq i \leq 2$, $3 \leq k \leq m$. Thus h fixes the subspaces $U := \langle b_1, b_2 \rangle$ and $U' := \langle b_3, \ldots, b_n \rangle$ in its action on W, and hence $\mathrm{Soc}(H)_w \leq \mathrm{Soc}(H)_{U,U'}$.

We claim that, when n is even, no $h \in \mathrm{Soc}(H)$ maps w to $w + u$. Suppose on the contrary that $h = (\alpha_{ij})$ is such an element. For $k \geq 3$, we define X_k and X_k^* as above. Now $X_k \neq \emptyset$ and $X_k^* \neq \emptyset$ because otherwise the coefficient of $b_k \otimes b_k^*$ in wh would be 0. Suppose that $|X_k| = 1$, say $X_k = \{a\}$. Then by (11), for any $\ell \neq k$, the coefficient of $b_k \otimes b_\ell^*$ in wh is $\alpha_{3-a,\ell}$ and this must be 0. Choose an $m \geq 3$, $m \neq k$ (such an m exists because $n > 2$ and n is even). We have $\alpha_{3-a,m}^* = 0$ and $X_m^* \neq \emptyset$, so $\alpha_{a,m}^* \neq 0$. Then (11) implies that $\alpha_{3-a,\ell} = 0$ for all $\ell \neq m$. However, this contradicts (9) for $i = j = 3 - a$. Thus $X_k = \{1, 2\}$ for all $k \geq 3$. Reversing the role of (α_{ij}) and (α_{ij}^*), the same argument proves that $X_k^* = \{1, 2\}$ for all $k \geq 3$. Hence the coefficient of $b_k \otimes b_k^*$ in wh is $\alpha_{1k}\alpha_{2k}^* + \alpha_{2k}\alpha_{1k}^* = 1 + 1 = 0$, which is a contradiction. This proves the claim.

For later use, we emphasize that the argument in the previous two paragraphs did not use the fact that the α_{ij} are elements of GF(2) until the very last step (to reach a contradiction in the case $|X_k| = |X_k^*| = 2$ for all $k \geq 3$). Instead, it utilized only the fact that the α_{ij} satisfy (9)–(11). So far we have proved that $M_{12,21} \cap \mathrm{Soc}(H)$ fixes

$U \le W$ and $U' \le W$. As noted above $w\tau = w$. Moreover, since $h^\tau = (h^{-1})^{\mathrm{tr}}$ for $h \in \mathrm{Soc}(H)$, τ normalizes $\mathrm{Soc}(H)_{U,U'}$. An easy computation in $\mathrm{SL}(2,2)$ shows that the group induced by $M_{12,21} \cap \mathrm{Soc}(H)$ on U is isomorphic to Z_2. Hence $M_{12,21} \cap \mathrm{Soc}(H)$ is a proper subgroup of $\mathrm{Soc}(H)_{U,U'}$. If $H = \mathrm{Soc}(H)$ then $M_{12,21} < H_{U,U'} < H$, while if $H = \mathrm{Soc}(H).\langle\tau\rangle$ then $M_{12,21} < \mathrm{Soc}(H)_{U,U'}.\langle\tau\rangle < H$, and so in either case $M_{12,21}$ is not maximal in H.

Case 2: $\mathrm{Soc}(H) = \mathrm{PSU}(n,2)$ *with* $n \ge 4$. Generators for the adjoint module of $\mathrm{PSU}(4,2).2$ are available in `atlasrep` and from these we also constructed generators for $\mathrm{PSU}(4,2)$. We computed the orbits of these groups and checked that they do not act primitively on all orbits.

Suppose that $n \ge 5$ and let W be the natural module of $\mathrm{SL}(n,4)$ with basis $B = \{b_1,\dots,b_n\}$. For $h = (\alpha_{ij}) \in \mathrm{SL}(n,4)$, we define $\overline{h} := (\alpha_{ij}^2)$. The group $\mathrm{SU}(n,2)$ in its action on W is defined as the subgroup of all matrices $h \in \mathrm{SL}(n,4)$ satisfying

$$h^{-1} = \overline{h}^{\mathrm{tr}}. \tag{13}$$

We define W^*, B^*, $W \otimes W^*$, $B \otimes B^*$, and (α_{ij}^*) as in Case 1. The elements $\alpha_{ij}, \alpha_{ij}^* \in \mathrm{GF}(4)$ satisfy (9) and (10). In addition, because of (13), if $h = (\alpha_{ij}) \in \mathrm{SU}(n,2)$ then for all i, j

$$\alpha_{ij}^* = \alpha_{ij}^2. \tag{14}$$

The action of $\mathrm{Soc}(H)$ on $W \otimes W^*$ is defined by (11). If the group $H = \mathrm{PSU}(n,2).2$ and $\sigma \in H$ conjugates all $h \in \mathrm{Soc}(H)$ to $h^\sigma = \overline{h}$ then by (14), h^σ is the inverse transpose of h. Hence the action of σ on $W \otimes W^*$ is defined, see (12), by $\sum_{i,j} \lambda_{ij} b_i \otimes b_j^* \mapsto \sum_{i,j} \lambda_{ij}^2 b_j \otimes b_i^*$. We define $\widetilde{W}$ and u as above and the same argument as in Case 1 yields that $\widetilde{W}$ and $\langle u\rangle$ are H-invariant. Moreover, we define a $\mathrm{GF}(2)$-subspace $\widetilde{W}_0$ by

$$\widetilde{W}_0 := \left\{ w = \textstyle\sum_{i,j} \lambda_{ij} b_i \otimes b_j^* \in \widetilde{W} \mid \lambda_{ji} = \lambda_{ij}^2 \text{ for all } i, j \right\}.$$

Let ω be a generator of $\mathrm{GF}(4)^*$. Then $\widetilde{W}_0$ has a $\mathrm{GF}(2)$-basis $\mathbb{B}$ of size n^2-1 consisting of the $\binom{n}{2}$ vectors $b_i \otimes b_j^* + b_j \otimes b_i^*$ for $i < j$, the $\binom{n}{2}$ vectors $\omega b_i \otimes b_j^* + \omega^2 b_j \otimes b_i^*$ for $i < j$, and the $n-1$ vectors $b_1 \otimes b_1^* + b_i \otimes b_i^*$ for $i \ge 2$. We claim that $\widetilde{W}_0$ is H-invariant. If $h = (\alpha_{ij}) \in \mathrm{Soc}(H)$ then by (11) for any i, j, k, ℓ the coefficients of $b_k \otimes b_\ell^*$ and $b_\ell \otimes b_k^*$ in $(b_i \otimes b_j^* + b_j \otimes b_i^*)h$ are $\alpha_{ik}\alpha_{j\ell}^* + \alpha_{jk}\alpha_{i\ell}^*$ and $\alpha_{i\ell}\alpha_{jk}^* + \alpha_{j\ell}\alpha_{ik}^*$, respectively and by (14) these coefficients are the squares of each other. Thus $(b_i \otimes b_j^* + b_j \otimes b_i^*)h \in \widetilde{W}_0$. Similarly, the coefficients of $b_k \otimes b_\ell^*$ and $b_\ell \otimes b_k^*$ in $(\omega b_i \otimes b_j^* + \omega^2 b_j \otimes b_i^*)h$ are $\omega\alpha_{ik}\alpha_{j\ell}^* + \omega^2\alpha_{jk}\alpha_{i\ell}^*$ and $\omega\alpha_{i\ell}\alpha_{jk}^* + \omega^2\alpha_{j\ell}\alpha_{ik}^*$, respectively and by (14) these coefficients are the squares of each other. Finally, the coefficients of $b_k \otimes b_\ell^*$ and $b_\ell \otimes b_k^*$ in $(b_1 \otimes b_1^* + b_i \otimes b_i^*)h$ are $\alpha_{1k}\alpha_{1\ell}^* + \alpha_{ik}\alpha_{i\ell}^*$ and $\alpha_{1\ell}\alpha_{1k}^* + \alpha_{i\ell}\alpha_{ik}^*$, respectively and by (14) these coefficients are the squares of each other. Thus h leaves $\widetilde{W}_0$ invariant. Moreover, σ fixes the basis vectors

$b_i \otimes b_j^* + b_j \otimes b_i^*$ and $b_1 \otimes b_1^* + b_i \otimes b_i^*$, and maps $\omega b_i \otimes b_j^* + \omega^2 b_j \otimes b_i^*$ to $\omega^2 b_i \otimes b_j^* + \omega b_j \otimes b_i^* = (b_i \otimes b_j^* + b_j \otimes b_i^*) + (\omega b_i \otimes b_j^* + \omega^2 b_j \otimes b_i^*) \in \widetilde{W}_0$. Thus σ fixes $\widetilde{W}_0$, and hence $\widetilde{W}_0$ is H-invariant, as claimed.

The adjoint module V of H is defined as the GF(2)-module $\widetilde{W}_0$ if n is odd, and as $\widetilde{W}_0/\langle u\rangle_{\mathrm{GF}(2)}$ if n is even. Define w, u, and $v \in V$ as in Case 1. We claim that the stabilizer $M_{12,21}$ of v is not maximal in H and so G is not extremely primitive. Now $w\sigma = w$ (by the σ-action described above), and hence $\sigma \in H_v$, so we need only consider elements of $\mathrm{Soc}(H)_v$.

If $h \in M_{12,21} \cap \mathrm{Soc}(H)$ then repeating verbatim the argument in Case 1, we obtain that h fixes $U = \langle b_1, b_2\rangle \le W$ and $U' = \langle b_3, \dots, b_n\rangle \le W$, provided we have a contradiction in the last line of proof (the case $wh = w + u$ and $|X_k| = |X_k^*| = 2$ for all $k \ge 3$). In this case, fix three different indices $k, \ell, m \ge 3$ (such indices exist because $n \ge 5$). Note that, by the assumptions in this last case, $\alpha_{ij} \ne 0$ for any $i \le 2$ and $j \in \{k, \ell, m\}$, and hence (using (14)), $\alpha_{ij}^{-1} = \alpha_{ij}^2 = \alpha_{ij}^*$. The coefficients of $b_k \otimes b_\ell^*, b_k \otimes b_m^*, b_\ell \otimes b_m^*$ in wh are $\alpha_{1k}\alpha_{2\ell}^* + \alpha_{2k}\alpha_{1\ell}^* = 0, \alpha_{1k}\alpha_{2m}^* + \alpha_{2k}\alpha_{1m}^* = 0$, and $\alpha_{1\ell}\alpha_{2m}^* + \alpha_{2\ell}\alpha_{1m}^* = 0$, respectively. From the first two equations we obtain $\alpha_{1\ell}^2\alpha_{2\ell} = \alpha_{1k}\alpha_{2k}^2 = \alpha_{1m}^2\alpha_{2m} \ne 0$, and from the third, $\alpha_{1\ell}\alpha_{2\ell}^2 = \alpha_{1m}^2\alpha_{2m} \ne 0$. These imply that $\alpha_{1j} = \alpha_{2j}$ for each $j \in \{k, \ell, m\}$. Hence the coefficient of $b_\ell \otimes b_\ell^*$ in wh is $\alpha_{1\ell}\alpha_{2\ell}^* + \alpha_{2\ell}\alpha_{1\ell}^* = 0$, which is a contradiction. Thus $M_{12,21} \cap \mathrm{Soc}(H) \le \mathrm{Soc}(H)_{U,U'}$.

The stabilizer of U and U' in $\mathrm{Soc}(H)$ acts as $\mathrm{SL}(2,2)$ on U, with generators

$$\begin{pmatrix} \omega & 0 \\ 0 & \omega^2 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

An easy calculation shows that $M_{12,21} \cap \mathrm{Soc}(H)$ acts as Z_2 on U (generated by the second matrix above). Hence $M_{12,21} \cap \mathrm{Soc}(H)$ is a proper subgroup of $\mathrm{Soc}(H)_{U,U'}$. As noted above, $w\sigma = w$. Also, since $h^\sigma = \bar{h} = (h^{-1})^{\mathrm{tr}}$ (by (13)) for all $h \in \mathrm{Soc}(H)$, σ normalizes $\mathrm{Soc}(H)_{U,U'}$. If $H = \mathrm{Soc}(H)$ then $M_{12,21} < H_{U,U'} < H$, while if $H = \mathrm{Soc}(H).\langle\sigma\rangle$ then $M_{12,21} < \mathrm{Soc}(H)_{U,U'}.\langle\sigma\rangle < H$, and so in either case $M_{12,21}$ is not maximal in H. □

We are now ready to prove the last assertion of Theorem 1.3

Theorem 4.7. *There are only finitely many finite extremely primitive groups of affine type that are not listed in Theorems* 1.2 *or* 1.3.

Proof. It is clear that for a fixed almost simple group H there are only finitely many d such that $G = Z_2^d.H$ is primitive, and that for a fixed d there are only finitely many almost simple groups H such that $G = Z_2^d.H$ is primitive. As a first consequence of this observation, we obtain that there are only finitely many extremely primitive groups $G = Z_2^d.H$ with $\mathrm{Soc}(H)$ sporadic.

Next, for $\mathrm{Soc}(H) = A_n$, the groups $Z_2^d.H$ with H acting on the deleted permutation module for the natural representation are listed in Theorems 1.2 or 1.3. By [10], if $n \geq 15$ then each faithful irreducible representation of H, apart from this deleted permutation module, has dimension at least $n(n-5)/2$. Now for n large enough, $n! < 2^{n(n-5)/4}$. Also, by [20], for n large enough A_n and S_n have less than $n!$ maximal subgroups. Hence, for large enough n, a primitive group $G = Z_2^d.H$ with $\mathrm{Soc}(H) = A_n$ and $d > n$ cannot be extremely primitive by Lemma 4.1.

Suppose next that H is of Lie type and the characteristic of H is odd. Examining the list of bounds for the minimal dimensions of cross-characteristic representations of Lie-type groups (originally in [15] and [27], with subsequent improvements listed in [29]), we see that if H acts irreducibly on $V = \mathrm{GF}(2)^d$ then $|H| < (2d)^{2(2+\log d)}$. Hence, for $|H|$ large enough, for any primitive $G = Z_2^d.H$ we have $|H|^{8/5} < 2^{d/2}$. Also, by [20], for $|H|$ large enough, H has less than $|H|^{8/5}$ maximal subgroups. Hence $G = Z_2^d.H$ cannot be extremely primitive by Lemma 4.1.

Suppose that H is of Lie type of even characteristic, and also (using [20]) suppose that $|H|$ is large enough such that the number of maximal subgroups of H is less than $|H|^{8/5}$. By Lemma 4.4 and the discussion following, if G is extremely primitive then H is defined over GF(2) and, apart from one group, V is a 2-restricted highest weight module for $\mathrm{Soc}(H)$. Classical groups H with rank at most 55 and exceptional groups give finitely many examples. If H is classical of rank $\ell \geq 55$ and $d \geq l^3/8$ then $2^{d/2} > |H|^{8/5}$ and G is not extremely primitive by Lemma 4.1. If $\ell \geq 55$ and $d < \ell^3/8$ then by [21, Theorem 5.1] the only possibilities for V are the natural, alternating square, and adjoint modules. The natural representation of H leads to the examples in Theorem 1.2 (b) (i) and Theorem 1.3 (c). Moreover, Lemmas 4.5 and 4.6 imply that there are only finitely many extremely primitive groups obtained from the alternating square and adjoint representations. □

This completes the proof of Theorem 1.3.

4.1. Commentary on completing the classification of affine extremely primitive groups. The unknown exceptions in Theorem 4.7 are due to the fact that we do not have a good bound on the number of maximal subgroups that is valid in *all* almost simple groups. A famous conjecture of G. E. Wall states that the number of maximal subgroups is at most $|H|$ in all groups H. The result of [20] quoted in the proof of Theorem 4.7 says that Wall's conjecture holds for A_n and S_n for large enough n. We also know that if $\mathrm{Soc}(H)$ is sporadic then H satisfies Wall's conjecture. Now consider the remaining case where $\mathrm{Soc}(H)$ is a Lie type simple group of rank r over a field of order q. It was proved recently by M. W. Liebeck, B. M. S. Martin and A. Shalev (see Theorem 1.3 of [18], together with the discussion following it) that the number of conjugacy classes of maximal subgroups of H is at most $cr^r \log\log q$ for some constant c. This number is at most $|H|^{o(1)}$, and each conjugacy class has size less than $|H|$. Hence the number of maximal subgroups of H is at most $|H|^{1+o(1)}$.

In anticipation of a full proof of Wall's conjecture for almost simple groups, we prove a stronger version of Theorem 4.7. *Let $\mathcal{S}$ be the family of almost simple groups satisfying Wall's conjecture.*

Theorem 4.8. *If $H \in \mathcal{S}$ and $G = Z_2^d.H$ is extremely primitive then either G is listed in Theorems* 1.2 *or* 1.3 *, or $(d, \mathrm{Soc}(H))$ is as in one of the lines of Table* 2.

Proof. We do a refined version of the proof of Theorem 4.7.

Table 2. Table for Theorem 4.8.

d	$\mathrm{Soc}(H)$	Conditions
40	$\mathrm{PSp}(4,9), \mathrm{SL}(5,2)$	two non-permutationally isomorphic groups for $\mathrm{SL}(5,2)$
48	$\mathrm{Sp}(8,2), \Omega^{\pm}(8,2)$	
70	$\mathrm{SL}(8,2), \mathrm{PSU}(8,2)$	
100	$\mathrm{Sp}(10,2)$	
126	$\mathrm{SL}(9,2)$	
$\binom{k}{3}$	$\mathrm{SL}(k,2)$	$7 \le k \le 14$
2^k	$\mathrm{Sp}(2k,2), \Omega^+(2k+2,2)$	$5 \le k \le 8$
27, 78	$\mathrm{E}_6(2)$	
78	${}^2\mathrm{E}_6(2)$	
56, 132	$\mathrm{E}_7(2)$	
248	$\mathrm{E}_8(2)$	

Case 1: $\mathrm{Soc}(H)$ *is sporadic.* In this case, the maximal subgroups of H are known [32], and we can use the exact number of maximal subgroups in the estimate of Lemma 4.1 to get an upper bound $d_1(H)$ on the dimension of the representations we have to consider. Also, the minimal dimension $d_2(H)$ of characteristic 2 representations is known [11]. In the twelve cases $\mathrm{Soc}(H) = \mathrm{Suz}, \mathrm{Fi}_{22}, \mathrm{Fi}_{23}, \mathrm{Fi}_{24}', \mathrm{He}, \mathrm{HN}, \mathrm{Th}, \mathrm{O'N}, \mathrm{Ly}, J_3, B, M$ we have $d_1(H) < d_2(H)$ so there are no extremely primitive examples. In the remaining cases, matrices for all representations of dimension at most $d_1(H)$ are available in [32] and `atlasrep` [31]. By Lemma 3.1, d-dimensional representations of the form $H \le \mathrm{GL}(d/2,4).2$ give no extremely primitive examples. In representations of dimension $d \le 22$, we simply computed all orbits of H on $V = \mathrm{GF}(2)^d$ and the permutation action of H on these orbits. We already described the handling of Co_1 in 24 dimensions in the proof of Lemma 4.2. These computations led to the examples in Lemma 4.2. The remaining cases are $(d, H) = (112, J_4)$ and $(28, \mathrm{Ru})$. In these two groups, generators for representatives of all conjugacy classes of maximal subgroups are available in [32] and `atlasrep`, so we could compute the exact value of

$|\mathrm{fix}(M)|$ for all maximal subgroups. This count, with an application of Lemma 4.1, proved that these remaining groups are not extremely primitive.

Case 2: $\mathrm{Soc}(H)$ *is alternating.* Suppose that $\mathrm{Soc}(H) = A_n$ and let $d_1(H) := 2\lceil \log n! \rceil$. Lemma 4.1 and our assumption $H \in \mathcal{S}$ implies that if $d > d_1(H)$ then $G = Z_2^d.H$ is not extremely primitive. The smallest nontrivial GF(2)-representation of H is the deleted permutation module, leading to extremely primitive groups in Theorems 1.2 (b) and 1.3 (b). By [10], if $n \geq 15$ then the second smallest representation has dimension at least $n(n-5)/2$. If $n \geq 17$ then $n(n-5)/2 > d_1(H)$ and so there are no further extremely primitive examples. For $n \leq 16$ the exact number of maximal subgroups is available, and Lemma 4.1 gives an upper bound on the dimension of representations we have to consider. We constructed the representations of dimension at most 20 and checked the orbit lengths of H on $V = \mathrm{GF}(2)^d$, leading (only) to the examples listed in Theorem 1.3. The only cases left were $(d, H) = (32, S_{11})$ and $(32, S_{12})$. In these cases, $H \leq \mathrm{GL}(16, 4).2$ and so Lemma 3.1 implies that $G = Z_2^d.H$ is not extremely primitive.

Case 3: $\mathrm{Soc}(H)$ *is Lie type of odd characteristic.* We proceed as in the proof of Theorem 4.7, just doing the estimates more precisely. In cross-characteristic representations $|H| < (2d)^{2(2+\log d)}$ so for $d > 2^{10}$ we have $|H| < 2^{d/2}$ and, by Lemma 4.1 and the assumption $H \in \mathcal{S}$, G is not extremely primitive. There are only finitely many H that have cross-characteristic representations of dimension at most 2^{10}. Most of these groups are eliminated by computing the exact value of $|H|$ and comparing it with $2^{d/2}$ for the minimal dimension d of a cross-characteristic representation. The remaining possibilities for $\mathrm{Soc}(H)$ are $\mathrm{PSL}(2, q)$ for $11 \leq q \leq 73$, $\mathrm{PSL}(3, 3)$, $\mathrm{PSL}(3, 5)$, $\mathrm{PSL}(4, 3)$, $\mathrm{PSp}(4, q)$ for $5 \leq q \leq 11$, $\mathrm{PSp}(6, 3)$, $\mathrm{PSp}(6, 5)$, $\mathrm{PSp}(8, 3)$, $\mathrm{PSp}(10, 3)$, $\mathrm{PSU}(3, 5)$, $\mathrm{PSU}(3, 7)$, $\mathrm{PSU}(4, 3)$, $\mathrm{PSU}(5, 3)$, and $G_2(3)$ (because of the isomorphisms $\mathrm{PSL}(2, 5) \cong \mathrm{PSL}(2, 4)$, $\mathrm{PSL}(2, 7) \cong \mathrm{PSL}(3, 2)$, $\mathrm{PSp}(4, 3) \cong \mathrm{PSU}(4, 2)$, and $\mathrm{PSU}(3, 3) \cong G_2(2)'$, we consider these groups to be defined in even characteristic and we consider $\mathrm{PSL}(2, 9) \cong A_6$ as an alternating group).

Suppose first that $\mathrm{Soc}(H) = \mathrm{PSL}(2, q)$, for some q with $11 \leq q \leq 73$. The exact number of maximal subgroups of H is known, and using this number in the estimate of Lemma 4.1 we get an upper bound $d_1(H)$ for the dimension of representations we have to consider. In all cases, $d_1(H) < 2(q-1)$; if $q \geq 23$ then $d_1(H) < q-1$; and if $q \geq 61$ then $d_1(H) < (q-1)/2$. If $11 \leq q \leq 19$ then all representations of dimension less than $2(q-1)$ actually have dimension at most 20. We have constructed all such representations (as factors of the tensor square of the permutation module of dimension $q+1$), computed all orbit lengths of H and verified that H acts primitively on each of its orbits only in the case $d = 8$, $H = \mathrm{PSL}(2, 17)$. This appears in Theorem 1.3 (c). For $q \geq 23$, the only even characteristic representation of H of dimension less than $q-1$ is of dimension $(q-1)/2$, and hence $d = (q-1)/2$ and $q \leq 59$. If $q \equiv 3, 5 \bmod 8$ then the $(q-1)/2$-dimensional representation is over GF(4) which is not extremely primitive by Lemma 3.1. For $q \equiv 1, 7 \bmod 8$ and

$23 \leq q \leq 41$, we constructed the $(q-1)/2$-dimensional representation of $\mathrm{Soc}(H)$, and computed the orbit lengths. In each case there are vectors $v \in V$ whose stabilizer is not maximal in $\mathrm{Soc}(H)$. This implies that the stabilizer of v is not maximal in H because for any maximal $M < H$ we have $M \cap \mathrm{Soc}(H)$ maximal in H. Finally, in the cases $q = 47, 49$, in the $(q-1)/2$-dimensional representations we found vectors v whose stabilizer is trivial in $\mathrm{Soc}(H)$ by a random search.

In the remaining cases, if $\mathrm{Soc}(H)$ is special linear, unitary, or $G_2(3)$ then we use the exact number of maximal subgroups of H in Lemma 4.1 to get an upper bound $d_1(H)$ for the dimension of representations we have to consider. In the cases where $\mathrm{Soc}(H) = \mathrm{PSL}(3,5)$, $\mathrm{PSU}(3,7)$, and $\mathrm{PSU}(5,3)$, $d_1(H)$ is less than the minimal dimension of a characteristic two representation and so no extremely primitive examples arise. If $\mathrm{Soc}(H) = \mathrm{PSL}(3,3)$ or $G_2(3)$, the only representations to consider have dimensions 12 and 14, respectively. Generators for all possible H are available in `atlasrep` and we computed all orbits of H and found ones on which H does not act primitively. If $\mathrm{Soc}(H) = \mathrm{PSL}(4,3)$ then only $d = 26$ is possible. We constructed the representation of $\mathrm{Soc}(H)$ by restricting the integer representation in `atlasrep` to GF(2) and by random search found $v \in V$ whose stabilizer has order 16. Since $|\mathrm{Out}(\mathrm{PSL}(4,3))| = 4$, this means that the stabilizer H_v of v is a proper subgroup of a Sylow 2-subgroup of H and so it is not maximal. If $\mathrm{Soc}(H) = \mathrm{PSU}(3,5), \mathrm{PSU}(4,3)$ then only $d = 20$ is possible. We constructed the representation of $\mathrm{Soc}(H)$ (from the GF(2)-representation of $\mathrm{PSU}(3,5).2$ and as a composition factor of the restriction of the 21-dimensional integer representation of $\mathrm{PSU}(4,3)$, respectively, both of these available in `atlasrep`). In the case $\mathrm{Soc}(H) = \mathrm{PSL}(3,5)$, there are vectors with stabilizers of order 2 and so their stabilizers are not maximal in H. In the case $\mathrm{Soc}(H) = \mathrm{PSU}(4,3)$, there are vectors with stabilizer of size 16. Since $|\mathrm{Out}(\mathrm{PSU}(4,3))| = 8$, again H_v is a proper subgroup of a Sylow 2-subgroup of H and so is not maximal.

Finally, in the cases where $\mathrm{Soc}(H) = \mathrm{PSp}(2n,q)$, [8] (see also [29, Section 4.3]) implies that the only irreducible GF(2)-representations satisfying $|H| < 2^{d/2}$ are of dimension $(q^n-1)/2$ or q^n-1, the latter occurring when the $(q^n-1)/2$-dimensional representations (the so-called Weyl modules) are over GF(4). However, it follows from Lemma 3.1 that the (q^n-1)-dimensional representations do not lead to extremely primitive examples. Out of the eight cases for $\mathrm{Soc}(H) = \mathrm{PSp}(2n,q)$ under consideration, the only two where the Weyl modules are defined over GF(2) are $(d, \mathrm{Soc}(H)) = (24, \mathrm{PSp}(4,7))$ and $(40, \mathrm{PSp}(4,9))$. We constructed the 24-dimensional modules for $\mathrm{PSp}(4,7)$ and in the fixed point space of an element of order 5 found a vector whose stabilizer has order 60, which cannot be maximal. The last case $(d, \mathrm{Soc}(H)) = (40, \mathrm{PSp}(4,9))$ is listed in the statement of Theorem 4.8 as a candidate leading to an extremely primitive permutation group.

Case 4: $\mathrm{Soc}(H)$ *is Lie type of even characteristic*. As discussed after Lemma 4.4, it is enough to consider the case that H is defined over GF(2), and either V is a

2-restricted highest weight module of $\mathrm{Soc}(H)$, or $\mathrm{Soc}(H) = {}^2F_4(2)'$ and $\dim V$ is 26 or 246. As in the previous cases, we use Lemma 4.1 and our assumption that $H \in \mathcal{S}$ to obtain the upper bound $d_1(H) := 2\lceil \log |H| \rceil$ for the dimension of representations that may lead to extremely primitive examples. If H is classical of rank n then $d_1(H)$ is a quadratic function of n. In particular, if $n > 16$ then $d_1(H) < n^3/8$ and if $n > 11$ then $d_1(H) < n^3$. However, [21, Theorem 5.1] states that if $n > 11$ then the only absolutely irreducible representations of dimension less than $n^3/8$ in the special linear and unitary cases are the trivial, natural, alternating square, and adjoint representations and the only absolutely irreducible representations of dimension less than n^3 in the symplectic and orthogonal cases are the trivial, natural, and alternating square representations. The extremely primitive groups obtained from the natural representations are listed in Theorems 1.2 (b) and 1.3 (c), and by Lemmas 4.5 and 4.6, the alternating square and adjoint representations also lead only to extremely primitive permutation groups listed in these theorems. If $n \leq 16$ in the special linear and unitary cases, or $n \leq 11$ in the symplectic and orthogonal cases, then the representations of $\mathrm{Soc}(H)$ of dimension less than $d_1(H)$ are listed in [21]. We listed the representations of dimension d with $20 < d < d_1(H)$ in the statement of Theorem 4.8 as candidates leading to extremely primitive examples. The remaining small-dimensional cases (excluding the natural, alternating square and adjoint representations, and their duals) are $(d, \mathrm{Soc}(H)) = (20, \mathrm{SL}(4,2)), (20, \mathrm{SL}(6,2)), (20, \mathrm{PSU}(6,2)), (16, \Omega^+(10,2))$, and the symplectic cases $(8, \mathrm{Sp}(6,2))$ and $(16, \mathrm{Sp}(8,2))$. In these cases, we constructed the H-module using `atlasrep` and computed all orbit lengths of H. The only case when H acts primitively on all of its orbits is $(d, H) = (8, \mathrm{Sp}(6,2))$ (listed in Theorem 1.3 (c)).

Similarly, if H is exceptional then all representations of dimension less than $d_1(H) := 2\lceil \log |H| \rceil$ are listed in [21]. The representations of dimension d with $26 < d < d_1(H)$ are listed in the statement of Theorem 4.8. The remaining cases are $(d, \mathrm{Soc}(H)) = (14, G_2(2)'), (26, {}^3D_4(2)), (26, F_4(2))$, and $(26, {}^2F_4(2)')$. In all of these cases, the H-modules are available in `atlasrep`. In the case where $(d, \mathrm{Soc}(H)) = (14, G_2(2)')$, we computed the lengths of all H-orbits and verified that H does not act primitively on all of them. The 26-dimensional modules are too big for the computation of all H-orbits. In the cases $H = {}^3D_4(2)$ and ${}^3D_4(2).3$, elements of order 28 have two-dimensional fixed point spaces. Two of the fixed vectors are in H-orbits of length 72×819 so their stabilizer is not maximal in H. In the case $H = F_4(2)$, elements of order 30 have two-dimensional fixed point spaces. One of the fixed vectors is in an H-orbit of length 256×69615 so its stabilizer is not maximal in H. In the cases $H = {}^2F_4(2)'$ and ${}^2F_4(2)$, elements of order 16 have two-dimensional fixed point spaces and at least two fixed vectors are in H-orbits of length 80×1755 so their stabilizers are not maximal in H. □

References

[1] M. Aschbacher, On the maximal subgroups of the finite classical groups. *Invent. Math.* **76** (1984), 469–514. Zbl 0537.20023 MR 746539

[2] P. J. Cameron, *Permutation Groups*. London Math. Soc. Stud. Texts 45, Cambridge University Press, Cambridge 1999. Zbl 0922.20003 MR 1721031

[3] L. E. Dickson, *Linear groups with an exposition of the Galois field theory*. B.G. Teubner, Leipzig 1901; Dover, New York 1958. Zbl 0082.24901 MR 104735

[4] J. D. Dixon and B. Mortimer, *Permutation groups*. Grad. Texts in Math. 163, Springer-Verlag, New York 1996. Zbl 0951.20001 MR 1409812

[5] W. Feit and G. M. Seitz, On finite rational groups and related topics. *Illinois J. Math.* **33** (1989), 103–131. Zbl 0701.20005 MR 974014

[6] The GAP Group, *GAP – Groups, algorithms, and programming, Version* 4.4.9, 2006. http://www.gap-system.org

[7] D. Gorenstein, Finite groups the centralizers of whose involutions have normal 2-complements. *Canad. J. Math.* **21** (1969), 335–357. Zbl 0201.03202 MR 0242939

[8] R. M. Guralnick, K. Magaard, J. Saxl, and P. H. Tiep, Cross characteristic representations of symplectic and unitary groups. *J. Algebra* **257** (2002), 291–347. Zbl 1025.20002 MR 1947325

[9] J. E. Humphreys, Modular representations of finite groups of Lie type. In *Finite Simple Groups II* (ed. M. J. Collins), Academic Press, London 1980, 259–290. Zbl 0472.20015 MR 0606048

[10] G. D. James, On the minimal dimensions of irreducible representations of symmetric groups. *Math. Proc. Cambridge Philos. Soc.* **94** (1983), 417–424. Zbl 0544.20011 MR 720791

[11] C. Jansen, The minimal degrees of faithful representations of the sporadic simple groups and their covering groups. *LMS J. Comput. Math.* **8** (2005), 122–144. Zbl 1089.20006 MR 2153793

[12] C. Jansen, K. Lux, R. Parker, and R. Wilson, *An atlas of Brauer characters*. Clarendon Press, Oxford 1995. Zbl 0831.20001 MR 1367961

[13] P. Kleidman and M. W. Liebeck, *The subgroup structure of the finite classical groups*. London Math. Soc. Lecture Note Ser. 129, Cambridge University Press, Cambridge 1990. Zbl 0697.20004 MR 1057341

[14] L. G. Kovács, Primitive subgroups of wreath products in product action. *Proc. London Math. Soc.* (3) **58** (1989), 306–322. Zbl 0671.20002 MR 977479

[15] V. Landazuri and G. M. Seitz, On the minimal degrees of projective representations of the finite Chevalley groups. *J. Algebra* **32** (1974), 418–443. Zbl 0325.20008 MR 0360852

[16] M. W. Liebeck, On the orders of maximal subgroups of the finite classical groups. *Proc. London Math. Soc.* (3) **50** (1985), 426–446. Zbl 0591.20021 MR 779398

[17] M. W. Liebeck, The affine permutation groups of rank three. *Proc. London Math. Soc.* (3) **54** (1987), 477–516. Zbl 0621.20001 MR 879395

[18] M. W. Liebeck, B. M. S. Martin, and A. Shalev, On conjugacy classes of maximal subgroups of finite simple groups, and a related zeta function. *Duke Math. J.* **128** (2005), 541–557. Zbl 1103.20010 MR 2145743

[19] M. W. Liebeck, C. E. Praeger and J. Saxl, On the O'Nan–Scott Theorem for finite primitive permutation groups. *J. Austral. Math. Soc. Ser. A* **44** (1988), 389–396. Zbl 0647.20005 MR 929529

[20] M. W. Liebeck and A. Shalev, Maximal subgroups of symmetric groups. *J. Combin. Theory Ser. A* **75** (1996), 341–352. Zbl 0866.20003 MR 1401008

[21] F. Lübeck, Small degree representations of finite Chevalley groups in defining characteristic. *LMS J. Comput. Math.* **4** (2001), 135–169. Zbl 1053.20008 MR 1901354

[22] W. A. Manning, Simply transitive primitive groups. *Trans. Amer. Math. Soc.* **29** (1927), 815–825. JFM 53.0108.01 MR 1501415

[23] D. V. Pasechnik and C. E. Praeger, On transitive permutation groups with primitive subconstituents. *Bull. London Math. Soc.* **31** (1999), 257–268. Zbl 0940.20004 MR 1673405

[24] D. S. Passman, Solvable $3/2$-transitive permutation groups. *J. Algebra* **7** (1967), 192–207. Zbl 0244.20005 MR 0235018

[25] D. S. Passman, Exceptional $3/2$-transitive permutation groups. *Pacific J. Math.* **29** (1969), 669–713. Zbl 0177.03701 MR 0244363

[26] G. Schlichting, Operationen mit periodischen Stabilisatoren. *Arch. Math.* **34** (1980), 97–99. Zbl 0449.20004 MR 583752

[27] G. M. Seitz and A. E. Zalesskii, On the minimal degrees of projective representations of the finite Chevalley groups, II. *J. Algebra* **158** (1993), 233–243. Zbl 0789.20014 MR 1223676

[28] M. Suzuki, On a finite group with a partition. *Arch. Math.* **12** (1961), 241–254. Zbl 0107.25902 MR 0136647

[29] P. H. Tiep, Low dimensional representations of finite quasisimple groups. In *Groups, combinatorics & geometry* (Durham, 2001), World Scientific, Singapore 2003, 277–294. Zbl 1032.20008 MR 1994973

[30] H. Wielandt, *Finite permutation groups*. Academic Press, New York 1964. Zbl 0138.02501 MR 183775

[31] R. A. Wilson, R. A. Parker, J. Bray, and T. Breuer, *AtlasRep*, a GAP package, version 1.3. http://www.math.rwth-aachen.de/ Thomas.Breuer/atlasrep/

[32] R. A. Wilson et al., ATLAS of finite group representations, version 3. http://brauer.maths.qmul.ac.uk/Atlas/v3/

Received February 6, 2007; revised March 26, 2007

A. Mann, Einstein Institute of Mathematics Givat Ram, The Hebrew University of Jerusalem, Jerusalem, 91904, Israel
E-mail: mann@math.huji.ac.il

C. E. Praeger, School of Mathematics and Statistics, The University of Western Australia, 35 Stirling Highway, Crawley, WA 6009, Australia

E-mail: praeger@maths.uwa.edu.au

Á. Seress, Department of Mathematics, The Ohio State University, Columbus, Ohio 43210, U.S.A.

E-mail: akos@math.ohio-state.edu