

ON SOLVABLE FACTORS OF ALMOST SIMPLE GROUPS

TIMOTHY C. BURNES AND CAI HENG LI

ABSTRACT. Let G be a finite almost simple group with socle G_0 . A (nontrivial) factorization of G is an expression of the form $G = HK$, where the factors H and K are core-free subgroups. There is an extensive literature on factorizations of almost simple groups, with important applications in permutation group theory and algebraic graph theory. In a recent paper, Li and Xia describe the factorizations of almost simple groups with a solvable factor H . Several infinite families arise in the context of classical groups and in each case a solvable subgroup of G_0 containing $H \cap G_0$ is identified. Building on this earlier work, in this paper we compute a sharp lower bound on the order of a solvable factor of every almost simple group and we determine the exact factorizations with a solvable factor. As an application, we describe the finite primitive permutation groups with a nilpotent regular subgroup, extending classical results of Burnside and Schur on cyclic regular subgroups, and more recent work of Li in the abelian case.

1. INTRODUCTION

A group G is said to be *factorizable* if there exist proper subgroups H and K such that $G = HK$. Such an expression is called a *factorization* of G and H, K are called its *factors*. We say that $G = HK$ is a *maximal* factorization if both factors are maximal subgroups of G , and it is an *exact* factorization if $H \cap K = 1$. Factorizations arise naturally in permutation group theory; if $G \leq \text{Sym}(\Omega)$ is a transitive permutation group with point stabilizer K , then a subgroup $H \leq G$ is transitive on Ω if and only if $G = HK$. Moreover, H is regular if and only if the factorization is exact.

In this paper, we are interested in factorizations of almost simple groups (recall that a finite group G is *almost simple* if $G_0 \leq G \leq \text{Aut}(G_0)$ for a nonabelian simple group G_0). In this setting, we say that a factorization $G = HK$ is *nontrivial* if both factors are core-free subgroups of G (that is, neither H nor K contains the socle G_0). The problem of determining the (nontrivial) factorizations of almost simple groups has a long history and numerous applications. For example, Itô [11] determined the factorizations of $\text{PSL}_2(q)$, and the exact factorizations of alternating and symmetric groups were classified by Wiegold and Williams [26], and later Liebeck, Praeger and Saxl described the general factorizations of these groups (see [21, Theorem D]). The factorizations of almost simple groups with socle an exceptional group of Lie type are determined in [10].

The maximal factorizations of all almost simple groups were classified by Liebeck, Praeger and Saxl [21] and this landmark paper from 1990 has been the foundation for more recent progress on the general problem. For example, Guralnick and Saxl [8, Theorem 3.1] apply [21] to describe the factorizations $G = HK$ of an almost simple group such that $H/O_p(H)$ is cyclic for some prime p , and they use this to study the structure of monodromy groups of polynomials. In a different direction, Giudici [7] works with [21] to identify the factorizations of almost simple groups with socle a sporadic simple group. Much more recently, Li and Xia [19] have used [21] to determine the factorizations of almost simple groups with the property that one of the factors has at least two non-solvable composition factors.

Factorizations of almost simple groups have many natural applications, especially when combined with the O’Nan-Scott Theorem, which describes the structure and action of finite primitive permutation groups. For example, see [2, 17, 23, 24] for related work on primitive groups containing transitive subgroups with prescribed properties, and we refer the reader to [18, 22] for applications to the study of Cayley graphs.

Let G be an almost simple group with socle G_0 . The general problem of determining the factorizations $G = HK$ with H solvable is investigated in depth by Li and Xia in [20] (as noted above, a special case of this problem was studied in earlier work by Guralnick and Saxl [8, Theorem 3.1]). Their main result, [20, Theorem 1.1], describes the possibilities for G , H and K , and the proof treats each family of almost simple groups in turn. By [10], there are no such factorizations if G_0 is an exceptional group of Lie type, and it is straightforward to read off the cases that arise when G_0 is a sporadic simple group via [7]. For alternating and symmetric groups, the analysis combines [21] with earlier work of Kantor [13] on k -homogeneous groups. In particular, if G_0 is non-classical, then Li and Xia give a detailed description of the triples (G, H, K) that arise.

Determining the factorizations of an almost simple classical group with a solvable factor is more difficult. Here [20, Theorem 1.1] states that if G is such a group with socle G_0 , then $G = HK$ with H solvable only if one of the following holds:

- I. $(G_0, H \cap G_0, K \cap G_0)$ belongs to one of 9 infinite families listed in [20, Table 1.1];
- II. $(G_0, H \cap G_0, K \cap G_0)$ is one of 28 “sporadic” cases recorded in [20, Table 1.2];
- III. Both H and K are solvable and (G, H, K) is described in [20, Proposition 4.1] (using earlier work of Kazarin [14]); here one infinite family arises (with $G_0 = \text{PSL}_2(q)$), together with 11 “sporadic” cases listed in [20, Table 4.1].

In order to describe the infinite families in [20, Table 1.1], Li and Xia identify specific subgroups A and B of G_0 (with A solvable) such that

$$H \cap G_0 \leq A, \quad K \cap G_0 \geq B,$$

and in every case they demonstrate the existence of an almost simple group G with socle G_0 and a factorization $G = HK$ satisfying the given conditions. For the reader’s convenience, the infinite families are listed in Table 1, together with the subgroups A and B (here P_k denotes the stabilizer of a k -dimensional totally singular subspace of the natural module for G_0). Similarly, a solvable subgroup A of G_0 with $H \cap G_0 \leq A$ is recorded for each of the factorizations in [20, Table 1.2], together with the structure of $K \cap G_0$ (as before, in every case there is a genuine factorization of an almost simple group G satisfying the given conditions). In view of the above, we will refer to Type I, II and III factorizations of an almost simple classical group, accordingly.

With applications in mind, it is desirable to extend [20, Theorem 1.1] by obtaining more information on the Type I factorizations of almost simple classical groups. In particular, we would like to shed more light on the minimal possibilities for a solvable factor in these cases (cf. [20, Problem 1.7]).

Our first result gives a sharp lower bound on the order of a solvable factor in every Type I factorization. In the statement, a *Type I.j factorization* refers to a factorization satisfying the conditions of Case j in Table 1.

Theorem 1. *Let G be an almost simple classical group with socle G_0 and suppose $G = HK$ is a Type I.j factorization of G . Then there exists an integer ℓ and an almost simple group G_1 with socle G_0 such that*

- (i) $G_1 = H_1K_1$ is a Type I.j factorization of G_1 ; and
- (ii) $|H_1| = \ell$ divides $|H|$,

where (G_1, H_1, K_1, ℓ) is listed in Table 2.

Case	G_0	A	B	Conditions
1	$\mathrm{PSL}_n(q)$	$\frac{q^n-1}{(q-1)d}:n$	$q^{n-1}:\mathrm{SL}_{n-1}(q)$	$d = (n, q-1)$
2	$\mathrm{PSL}_4(q)$	$q^3:\frac{q^3-1}{d}:3 < P_k$	$\mathrm{PSp}_4(q)$	$\begin{cases} d = (4, q-1) \\ k \in \{1, 3\} \end{cases}$
3	$\mathrm{PSp}_{2m}(q)$	$q^{\frac{1}{2}m(m+1)}:(q^m-1).m < P_m$	$\Omega_{2m}^-(q)$	$m \geq 2, q$ even
4	$\mathrm{PSp}_4(q)$	$q^3:(q^2-1).2 < P_1$	$\mathrm{Sp}_2(q^2)$	q even
5	$\mathrm{PSp}_4(q)$	$q^{1+2}:\frac{q^2-1}{2}.2 < P_1$	$\mathrm{PSp}_2(q^2)$	q odd
6	$\mathrm{PSU}_{2m}(q)$	$q^{m^2}:\frac{q^{2m}-1}{(q+1)d}.m < P_m$	$\mathrm{SU}_{2m-1}(q)$	$\begin{cases} m \geq 2 \\ d = (2m, q+1) \end{cases}$
7	$\Omega_{2m+1}(q)$	$(q^{\frac{1}{2}m(m-1)}, q^m):\frac{q^m-1}{2}.m < P_m$	$\Omega_{2m}^-(q)$	$m \geq 3, q$ odd
8	$\mathrm{P}\Omega_{2m}^+(q)$	$q^{\frac{1}{2}m(m-1)}:\frac{q^m-1}{d}.m < P_k$	$\Omega_{2m-1}(q)$	$\begin{cases} m \geq 5 \\ d = (4, q^m-1) \\ k \in \{m, m-1\} \end{cases}$
9	$\mathrm{P}\Omega_8^+(q)$	$q^6:\frac{q^4-1}{d}.4 < P_k$	$\Omega_7(q)$	$\begin{cases} d = (4, q^4-1) \\ k \in \{1, 3, 4\} \end{cases}$

TABLE 1. The Type I factorizations of classical groups in [20, Table 1.1]

Remark 1. In Table 2, we use the same numbering of cases as in Table 1 and we assume all of the conditions stated in the final column of that table. In addition, we adopt the following conventions in Table 2:

- (a) It is convenient to allow $n = 2$ in Case 1, which is strictly speaking a Type III factorization as the parabolic subgroup is solvable (see [20, Proposition 4.1(a)]).
- (b) In Case 2, the group $G_1 \leq \mathrm{PGL}_4(q)$ is

$$G_1 = \begin{cases} \mathrm{PSL}_4(q).2 & \text{if } q \equiv 1 \pmod{4} \\ \mathrm{PSL}_4(q) & \text{otherwise.} \end{cases}$$

- (c) In Case 6, N_1 denotes the stabilizer in G_1 of a 1-dimensional nondegenerate subspace of the natural module.
- (d) In Case 7, we define $e = 2$ if $q^m \equiv 3 \pmod{4}$, otherwise $e = 1$. In addition, we write N_1^- for the stabilizer of a nondegenerate 1-space W such that W^\perp is of minus-type (that is, W^\perp has Witt index $m-1$).
- (e) In Cases 8 and 9, N_1 denotes the stabilizer of a 1-space U , where U is nondegenerate if q is odd and nonsingular if q is even.

Remark 2. It is interesting to compare the structure of the subgroups H_1 in Table 2 with the overgroup A of $H \cap G_0$ presented in Table 1. With the exception of Case 1, the overgroup A contains the full unipotent radical U of an appropriate parabolic subgroup of G_0 , but in most cases we find that only a small subgroup of U is needed to construct a solvable factor. Indeed, the main challenge in the proof of Theorem 1 is to determine how much of the unipotent radical needs to be included in a solvable factor. In this respect, it is worth highlighting Cases 2, 5 and 7, which are special in the sense that every solvable factor must contain the full unipotent radical (see the proofs of Propositions 2.2 and 2.8 for further details).

Next we turn to the problem of determining an absolute lower bound on the order of a solvable factor of any almost simple group with a given socle. Let G_0 be a nonabelian finite simple group and let

$$\mathcal{S}(G_0) = \{H : G = HK, H \text{ solvable, } K \text{ core-free, } \mathrm{soc}(G) = G_0\}$$

Case	G_1	H_1	K_1	ℓ
1	$\mathrm{PGL}_n(q)$	$\frac{q^n-1}{q-1}$	P_1	$\frac{q^n-1}{q-1}$
2	See Remark 1(b)	$q^3:\frac{q^3-1}{(2,q-1)}$	$\mathrm{PGSp}_4(q)$	$\frac{q^3(q^3-1)}{(2,q-1)}$
3	$\mathrm{Sp}_{2m}(q)$	$q^m:(q^m-1)$	$\mathrm{O}_{2m}^-(q)$	$q^m(q^m-1)$
4	$\mathrm{Sp}_4(q)$	$q^2:(q^2-1)$	$\mathrm{Sp}_2(q^2).2$	$q^2(q^2-1)$
5	$\mathrm{PGSp}_4(q)$	$q^{1+2}:(q^2-1)$	$\mathrm{PGSp}_2(q^2).2$	$q^3(q^2-1)$
6	$\mathrm{PGU}_{2m}(q)$	$q^{2m}:\frac{q^{2m}-1}{q+1}$	N_1	$\frac{q^{2m}(q^{2m}-1)}{q+1}$
7	$\mathrm{SO}_{2m+1}(q)$	$(q^{\frac{1}{2}m(m-1)}.q^m):\frac{q^m-1}{e}$	N_1^-	$\frac{1}{e}q^{\frac{1}{2}m(m+1)}(q^m-1)$
8	$\begin{cases} \Omega_{2m}^+(q) & q \text{ even} \\ \mathrm{PSO}_{2m}^+(q) & q \text{ odd} \end{cases}$	$q^m:\frac{q^m-1}{(2,q-1)}$	N_1	$\frac{q^m(q^m-1)}{(2,q-1)}$
9	$\begin{cases} \Omega_8^+(q) & q \text{ even} \\ \mathrm{PSO}_8^+(q) & q \text{ odd} \end{cases}$	$q^4:\frac{q^4-1}{(2,q-1)}$	N_1	$\frac{q^4(q^4-1)}{(2,q-1)}$

TABLE 2. Type I factorizations $G_1 = H_1K_1$ with $|H_1| = \ell$ in Theorem 1

be the set of solvable factors of almost simple groups with socle G_0 . Set

$$\ell(G_0) = \begin{cases} \min\{|H| : H \in \mathcal{S}(G_0)\} & \text{if } \mathcal{S}(G_0) \text{ is nonempty} \\ 0 & \text{otherwise.} \end{cases}$$

By inspecting [20], we see that $\mathcal{S}(G_0)$ is nonempty if and only if one of the following holds:

- (a) $G_0 \in \{A_n, \mathrm{PSL}_n(q), \Omega_{2m+1}(q), \mathrm{P}\Omega_{2m}^+(q), \mathrm{M}_{11}, \mathrm{M}_{12}, \mathrm{M}_{22}, \mathrm{M}_{23}, \mathrm{M}_{24}, \mathrm{J}_2, \mathrm{HS}, \mathrm{He}, \mathrm{Suz}\}$;
- (b) $G_0 = \mathrm{PSU}_n(q)$ and either n is even, or $n = 3$ and $q \in \{3, 5, 8\}$;
- (c) $G_0 = \mathrm{PSp}_{2m}(q)$ and either q is even, or $m = 2$, or $m = q = 3$.

By combining Theorem 1 with the analysis in [20], we can compute $\ell(G_0)$ precisely (see Remark 3.5 for comments on the analogous problem for abelian factors).

Theorem 2. *Let G_0 be a nonabelian finite simple group with $\ell(G_0) > 0$. Then $\ell(G_0)$ is recorded in Table 3, together with a triple (G, H, K) where $G = HK$ has socle G_0 , H is solvable, K is core-free and $|H| = \ell(G_0)$.*

Remark 3. Some comments on the information in Table 3 are in order.

- (a) For $G_0 = \Omega_{2m+1}(q)$, we define the integer $e \in \{1, 2\}$ as in Remark 1(d) and we take

$$G = \mathrm{SO}_{2m+1}(q), \quad H = (q^{\frac{1}{2}m(m-1)}.q^m):\frac{q^m-1}{e}, \quad K = N_1^-.$$

- (b) For $G_0 = \mathrm{P}\Omega_{2m}^+(q)$ we set $d = (2, q-1)$ and

$$G = \begin{cases} \Omega_{2m}^+(q) & q \text{ even} \\ \mathrm{PSO}_{2m}^+(q) & q \text{ odd,} \end{cases} \quad H = q^m:\frac{q^m-1}{d}, \quad K = N_1.$$

- (c) In the second row of the table, we have $G_0 = \mathrm{PSL}_2(q)$ with $q \geq 5$ and $q \neq 5, 7, 9, 11$. Note that $q \neq 5, 7, 9$ due to the existence of the exceptional isomorphisms $\mathrm{PSL}_2(5) \cong A_5$, $\mathrm{PSL}_2(7) \cong \mathrm{PSL}_3(2)$ and $\mathrm{PSL}_2(9) \cong A_6$. Similarly, we note the isomorphisms $\mathrm{PSL}_4(2) \cong A_8$ and $\mathrm{PSU}_4(2) \cong \mathrm{PSp}_4(3)$ (see [16, Proposition 2.9.1]).
- (d) For $G_0 = \mathrm{PSU}_4(3)$ we take $G = \mathrm{PSU}_4(3).2 < \mathrm{PGU}_4(3)$.

In [24], Liebeck, Praeger and Saxl determine the almost simple primitive permutation groups with a regular subgroup. In other words, they determine the exact nontrivial factorizations of almost simple groups with a maximal factor, and one can read off the examples with a solvable factor. Our next result describes the exact factorizations of

G_0	$\ell(G_0)$	G, H, K
A_n	n	S_n, C_n, S_{n-1}
$\text{PSL}_2(q), q \geq 5$ $q \neq 5, 7, 9, 11$	$q + 1$	$\text{PGL}_2(q), C_{q+1}, P_1$
$\text{PSL}_n(q), n \geq 3$ $(n, q) \neq (4, 2)$	$\frac{q^n - 1}{q - 1}$	$\text{PGL}_n(q), \frac{q^n - 1}{q - 1}, P_1$
$\text{PSU}_{2m}(q), m \geq 2$ $(m, q) \neq (2, 2), (2, 3), (2, 8)$	$\frac{q^{2m}(q^{2m} - 1)}{q + 1}$	$\text{PGU}_{2m}(q), q^{2m} : \frac{q^{2m} - 1}{q + 1}, N_1$
$\text{PSp}_{2m}(q), m \geq 2, q$ even $(m, q) \neq (2, 2)$	$q^m(q^m - 1)$	$\text{PSp}_{2m}(q), q^m : (q^m - 1), \text{O}_{2m}^-(q)$
$\text{PSp}_4(q), q \geq 5$ odd	$q^3(q^2 - 1)$	$\text{PGSp}_4(q), q^{1+2} : (q^2 - 1), \text{PGSp}_2(q^2).2$
$\Omega_{2m+1}(q), m \geq 3$	$\frac{1}{e} q^{\frac{1}{2}m(m+1)}(q^m - 1)$	See Remark 3(a)
$\text{P}\Omega_{2m}^+(q), m \geq 4$	$\frac{1}{d} q^m(q^m - 1)$	See Remark 3(b)
$\text{PSL}_2(7)$	7	$\text{PSL}_2(7), C_7, S_4$
$\text{PSL}_2(11)$	11	$\text{PSL}_2(11), C_{11}, A_5$
$\text{PSU}_3(3)$	216	$\text{PSU}_3(3), 3_+^{1+2}:8, \text{PSL}_2(7)$
$\text{PSU}_3(5)$	1000	$\text{PSU}_3(5), 5_+^{1+2}:8, A_7$
$\text{PSU}_3(8)$	513	$\text{PSU}_3(8).3^2, 57:9, 2^{3+6}:(63:3)$
$\text{PSU}_4(3)$	162	$\text{PSU}_4(3).2, 3^4:2, \text{PSL}_3(4).2$
$\text{PSU}_4(8)$	4617	$\text{PSU}_4(8).3, (513:3).3, (2^{12}.\text{SL}_2(64).7).3$
$\text{PSp}_4(3)$	27	$\text{PSp}_4(3), 3_+^{1+2}, 2^4:A_5$
M_{11}	11	M_{11}, C_{11}, M_{10}
M_{12}	12	M_{12}, D_{12}, M_{11}
M_{22}	22	$M_{22}.2, D_{22}, \text{PSL}_3(4).2$
M_{23}	23	M_{23}, C_{23}, M_{22}
M_{24}	24	M_{24}, S_4, M_{23}
J_2	100	$J_2.2, 5^2:4, G_2(2)$
HS	100	$\text{HS}.2, 5^2:4, M_{22}.2$
He	2058	$\text{He}.2, 7_+^{1+2}:6, \text{Sp}_4(4).4$
Suz	2916	$\text{Suz}.2, 3^5:12, G_2(4).2$

TABLE 3. The values of $\ell(G_0)$ in Theorem 2 and a factorization $G = HK$ with $\text{soc}(G) = G_0$ and $|H| = \ell(G_0)$

almost simple groups with a solvable factor in a more general setting, without assuming that one of the factors is maximal.

In Table 4 we write $\mathcal{O} \leq C_2$, and $\mathcal{O}_1, \mathcal{O}_2$ are subgroups of \mathcal{O} such that $\mathcal{O} = \mathcal{O}_1\mathcal{O}_2$. Also recall that a subgroup of S_n is *2-homogeneous* if it acts transitively on the set of subsets of $\{1, \dots, n\}$ of size 2.

Theorem 3. *Let G be an almost simple group with socle G_0 and $G = HK$ such that H is solvable, K is core-free and $H \cap K = 1$. Then one of the following holds:*

- (i) $G_0 = A_n$, H is transitive on $\{1, \dots, n\}$ and $K = A_{n-1}$ or S_{n-1} .
- (ii) $G_0 = A_n$, $n = p^a$ is a prime power, $H \leq \text{AGL}_1(p^a)$ is 2-homogeneous on $\{1, \dots, n\}$ and $A_{n-2} \trianglelefteq K \leq S_{n-2} \times S_2$.
- (iii) $G_0 = \text{PSL}_n(q)$, $H \cap G_0 \leq \frac{q^n - 1}{(q - 1)d} : n$ and $q^{n-1} : \text{SL}_{n-1}(q) \trianglelefteq K \cap G_0$ with $d = (n, q - 1)$.
- (iv) $G_0 = \text{PSp}_{2m}(q)$ with q even, $m \geq 3$, $H \cap G_0 \leq q^m : (q^m - 1).m$ and $K \cap G_0 = \Omega_{2m}^-(q)$.
- (v) (G, H, K) is one of the cases listed in Table 4.

Remark 4. Let us comment on the statement of Theorem 3.

- (a) As recorded in Table 5, there exist infinite families of exact factorizations satisfying the conditions in cases (i)–(iv). Note that in the final row of Table 5, we have $H = W:C < P_m$, where W is elementary abelian of order q^m and C is a Singer cycle in $\mathrm{GL}_m(q)$ that acts transitively on the nontrivial elements of W . In case (iv), we are not aware of an example with m even.
- (b) In Table 4, we have omitted any factorizations that are isomorphic to one of the examples in parts (i)–(iv). For instance, $G = S_6$ has an exact factorization $G = HK$ with $H \in \{C_6, D_6\}$ and $K = \mathrm{PGL}_2(5) \cong S_5$, which is included in part (i). Similarly, $G = A_8 \cong \mathrm{PSL}_4(2)$ has a factorization with $H = C_{15}$ and $K = \mathrm{AGL}_3(2)$, which is covered in part (iii).
- (c) Notice that there are several cases in Table 4 where both H and K are solvable. Here we record the triple (G, H, K) in the table, but we omit (G, K, H) .
- (d) Consider Case 19 in Table 4, with $G = \mathrm{PSL}_3(8).(3 \times \mathcal{O})$, $H = 73:(9 \times \mathcal{O})$ and $K = 2^{3+6}:7^2:3$. Then $G = HK$ is an exact factorization and H is a maximal subgroup of G , so we can view G as an almost simple primitive group with point stabilizer H and regular subgroup K . It is worth noting that this case has been omitted in the statement of [24, Theorem 1.1], which describes all the almost simple primitive groups with a regular subgroup.
- (e) In Case 25 of Table 4, $G = \mathrm{PSU}_4(3).2$ is the unique index-two subgroup of $\mathrm{PGU}_4(3)$. In Case 27, the group $G = \mathrm{PSU}_4(3).2^2$ contains an involutory graph automorphism with centralizer of type $\mathrm{Sp}_4(3)$, which distinguishes it from the group in Case 28 of the same shape.

In a sequel, we will use the main results in this paper to characterize the quasiprimitive permutation groups which contain a transitive solvable subgroup, extending classical results of Burnside and Schur on primitive groups with a transitive cyclic subgroup. As a first step in this direction, we present Theorem 4 below, which describes the finite primitive permutation groups with a regular nilpotent subgroup. This extends earlier work of Li [17] on primitive groups containing an abelian regular subgroup. In order to state this result, we need to introduce some new terminology.

Let H be a finite group. By considering the regular action, we may view H as a regular subgroup of a 2-transitive permutation group (namely, S_n acting on $\{1, \dots, n\}$, where n is the order of H). Following Wielandt, we say that H is a *Burnside-group* (in short, *B-group*) if every primitive permutation group containing a regular subgroup isomorphic to H is 2-transitive (see [27, Definition 25.1]). The term ‘B-group’ is due to the fact that Burnside [6] first proved that every cyclic group of composite prime-power order is a B-group (also see [29]). For more than a century, the problem of classifying B-groups and characterizing primitive groups with a regular subgroup has attracted considerable attention; we refer the reader to [27] for the early work and [2, 17, 23, 24] for more recent results.

For some special classes of groups, the above problems have been solved. For example, Schur [25] proved that every cyclic group of composite order is a B-group, and the primitive groups containing a cyclic regular subgroup are classified in [12]. More generally, the primitive groups with an abelian regular subgroup are determined in [17]. Note that a group of the form

$$H = H_1 \times H_2 \times \cdots \times H_d$$

with $|H_1| = \cdots = |H_d| = m \geq 3$ and $d \geq 2$ is not a B-group, since H is a regular subgroup of the simply primitive permutation group $S_m \wr S_d$ of degree m^d .

Case	G	H	K
1	$A_8.\mathcal{O}$	$AGL_1(8)$	$(A_5 \times 3).2.\mathcal{O}$
2	$A_8.\mathcal{O}$	$AFL_1(8)$	$S_5 \times \mathcal{O}$
3	A_{25}	$5^2:SL_2(3)$	A_{23}
4	S_{25}	$5^2:SL_2(3)$	$S_{23}, A_{23} \times 2$
5	$A_{32}.\mathcal{O}$	$AFL_1(32)$	$(A_{29} \times 3).2.\mathcal{O}$
6	A_{49}	$7^2:Q_8.S_3$	A_{47}
7	S_{49}	$7^2:Q_8.S_3$	$S_{47}, A_{47} \times 2$
8	$A_{121}.\mathcal{O}$	$11^2:SL_2(3).5.\mathcal{O}$	A_{119}
9	S_{121}	$11^2:SL_2(3).5$	$S_{119}, A_{119} \times 2$
10	A_{529}	$23^2:SL_2(3).22$	A_{527}
11	S_{529}	$23^2:SL_2(3).22$	$S_{527}, A_{527} \times 2$
12	$PSL_2(11).\mathcal{O}$	$11:\mathcal{O}$	A_5
13	$PSL_2(11).\mathcal{O}$	$11:(5 \times \mathcal{O}_1)$	$A_4.\mathcal{O}_2$
14	$PSL_2(23).\mathcal{O}$	$23:(11 \times \mathcal{O})$	S_4
15	$PSL_2(29)$	$29:7$	A_5
16	$PSL_2(59).\mathcal{O}$	$59:(29 \times \mathcal{O})$	A_5
17	$PSL_3(3).\mathcal{O}$	$13:(3 \times \mathcal{O})$	$AFL_1(9)$
18	$PTL_3(4).\mathcal{O}$	$7:(3 \times \mathcal{O}).S_3$	$2^4:(3 \times D_{10}).2$
19	$PSL_3(8).(3 \times \mathcal{O})$	$73:(9 \times \mathcal{O}_1)$	$2^{3+6}:7^2:(3 \times \mathcal{O}_2)$
20	$PGL_4(3)$	$(3^3:13:3).2$	$((4 \times PSL_2(9)):2).2$
21	$PSL_4(3).2^2$	$(3^3:13:3).2$	$((4 \times PSL_2(9)):2).2^2$
22	$PTL_4(4).\mathcal{O}$	$(2^6:63:3).2$	$((5 \times PSL_2(16)):2).2.\mathcal{O}$
23	$PSL_5(2).\mathcal{O}$	$31:(5 \times \mathcal{O})$	$2^6:(S_3 \times PSL_3(2))$
24	$PSU_3(8).3^2.\mathcal{O}$	$57:9.\mathcal{O}_1$	$2^{3+6}:(63:3).\mathcal{O}_2$
25	$PSU_4(3).2$	$3^4:2, 3^3.6, 3^3.D_6, 3_{\pm}^{1+2}.6, 3_{\pm}^{1+2}.D_6,$	$PSL_3(4).2$
26	$PGU_4(3)$	$3^4:4$	$PSL_3(4).2$
27	$PSU_4(3).2^2$	$3^4:2^2, 3^3.D_{12}, 3^3.(6 \times 2), 3^2.3^2.2^2$	$PSL_3(4).2$
28	$PSU_4(3).2^2$	$3^4:2, 3^3.6, 3^3.D_6, 3_{\pm}^{1+2}.6, 3_{\pm}^{1+2}.D_6$	$PSL_3(4).2^2$
29	$PSU_4(3).D_8$	$3^4:2^2, 3^4:4, 3^3.D_{12}, 3^3.(6 \times 2), 3^2.3^2.2^2$	$PSL_3(4).2^2$
30	$PSU_4(8).3.\mathcal{O}$	$(513:3).3.\mathcal{O}_1$	$(2^{12}.SL_2(64).7).3.\mathcal{O}_2$
31	$PSp_4(3).\mathcal{O}$	$3_{\pm}^{1+2}:\mathcal{O}_1$	$2^4:(A_5.\mathcal{O}_2)$
32	$PSp_4(3).\mathcal{O}$	$3_{\pm}^{1+2}:(Q_8.\mathcal{O}_1)$	$\mathcal{O}_2.S_5$
33	$PGSp_4(3)$	$2^4:5:4$	$3_{\pm}^{1+2}:S_3, 3^3:S_3$
34	$PGSp_6(3)$	$(3_{\pm}^{1+4}:2^{1+4}.D_{10}).2$	$PSL_2(27).6$
35	$\Omega_8^+(2).\mathcal{O}$	$2^6:15, 2^4:15.4$	$A_9.\mathcal{O}$
36	M_{11}	C_{11}	M_{10}
37	M_{11}	$11:5$	$(3^2:Q_8).2$
38	$M_{12}.\mathcal{O}$	$(3^2:Q_8).2$	$PSL_2(11).\mathcal{O}$
39	M_{12}	$C_6 \times C_2, A_4, D_{12}$	M_{11}
40	$M_{12}.2$	$S_4, D_{24}, D_8 \times 3, 3:D_8$	M_{11}
41	$M_{22}.2$	D_{22}	$PSL_3(4).2$
42	M_{23}	C_{23}	M_{22}
43	M_{23}	$23:11$	$PSL_3(4).2, 2^4:A_7$
44	M_{24}	$S_4, D_{24}, D_8 \times 3, 3:D_8, A_4 \times 2$	M_{23}
45	$J_2.2$	$5^2:4$	$G_2(2)$
46	$HS.2$	$5^2:4$	$M_{22}.2$
47	$He.2$	$7_{\pm}^{1+2}:6$	$Sp_4(4).4$

TABLE 4. The exact factorizations $G = HK$ in Theorem 3(v)

Case	G	H	K	Conditions
(i)	S_n	C_n	S_{n-1}	
(ii)	S_{p^a}	$\text{AGL}_1(p^a)$	S_{p^a-2}	
(iii)	$\text{PGL}_n(q)$	$\frac{q^n-1}{q-1}$	P_1	
(iv)	$\text{Sp}_{2m}(q)$	$q^m:(q^m-1)$	$\Omega_{2m}^-(q)$	$m \geq 3$ odd

TABLE 5. Some exact factorizations in parts (i)–(iv) of Theorem 3

Let $G \leq \text{Sym}(\Delta)$ be a primitive group with socle T and let d be a positive integer. Consider the primitive product action of $G \wr S_d$ on Δ^d . Then we refer to any primitive subgroup of $G \wr S_d$ with socle T^d as a *blow-up* of G on Δ (note that we allow $d = 1$). This leads us naturally to the following definition.

Definition. A finite group H is called a *generalized B-group* if every primitive permutation group containing a regular subgroup isomorphic to H is a blow-up of a 2-transitive group.

An elementary abelian p -group C_p^d is a regular subgroup of a primitive affine group, which may not be 2-transitive, and thus C_p^d is not a B-group, nor a generalized B-group, in general. More precisely, one can show that C_p^d is a B-group if and only if $p = 2$, $2^d - 1$ is a Mersenne prime and the only simple irreducible subgroups of $\text{GL}_d(2)$ are C_{2^d-1} and $\text{GL}_d(2)$ itself (see [29, Proposition 7.5]). For example, C_2^3 is a B-group.

We will also need the following definition.

Definition. Two groups are *class-mates* if they are isomorphic to regular subgroups of the same primitive permutation group, which is not a symmetric or alternating group in its natural action.

Note that if we allow the symmetric or alternating group in its natural action, then two groups would be class-mates if and only if they have the same order, so we exclude this situation in the definition.

By [17], every finite abelian group is either a generalized B-group or a class-mate of an elementary abelian p -group. The latter examples come from affine permutation groups; such a group contains a regular subgroup which is elementary abelian and normal, and it may also contain other regular subgroups. Indeed, a very nice construction of Hegedus [9] shows that if $d \geq 5$ then $\text{AGL}_d(p)$ has a regular subgroup which contains no nontrivial translations. In particular, two class-mates may intersect trivially.

Our main result on nilpotent regular subgroups of primitive groups is the following, which extends the main theorem of [17] on abelian regular subgroups. In the statement, we say that a primitive group is of *product-type* if it is the blow-up of an almost simple primitive group.

Theorem 4. *Let G be a finite primitive permutation group of degree n with socle T and let H be a nilpotent regular subgroup of G . Then one of the following holds:*

- (i) $T = A_n$ and H is a nilpotent group of order n .
- (ii) $G \leq \text{AGL}_d(p)$ is an affine group and H is a class-mate of $T = C_p^d$.
- (iii) G is a product-type group, $T = S^d$, $n = m^d$ and one of the following holds:
 - (a) H is a class-mate of C_m^d and (S, m) is one of (A_m, m) , $(\text{PSL}_a(q), \frac{q^a-1}{q-1})$, $(\text{PSL}_2(11), 11)$, $(M_{11}, 11)$ or $(M_{23}, 23)$.
 - (b) $S = M_{12}$ and H is a class-mate of $(C_6 \times C_2)^d$.
 - (c) $S = M_{24}$ and H is a class-mate of $(D_8 \times C_3)^d$.

(iv) G is a product-type group with $T = \mathrm{PSp}_4(3)^d$ and H is a class-mate of $(3_+^{1+2})^d$.

Remark 5. Consider the primitive group $G = \mathrm{PSp}_4(3) \wr S_d$ in its product action of degree 27^d . Here $(3_+^{1+2})^d$ is a regular subgroup of G , and so is $(3_-^{1+2})^d$. As explained in Example 5.7, if e, f are non-negative integers and $d = e + 3f$ then $(3_+^{1+2})^e \times (3^6 : 3_+^{1+2})^f$ is another regular subgroup. Since the action of $\mathrm{PSp}_4(3)$ on the cosets of $2^4 : A_5$ is simply primitive, it follows that H is *not* a generalized B-group in part (iv).

This leads to the following theorem, which shows that ‘most’ nilpotent groups are generalized B-groups and class-mates of homocyclic groups.

Theorem 5. *Let H be a finite nilpotent group. Then one of the following holds:*

- (i) H is a generalized B-group.
- (ii) H is a class-mate of an elementary abelian p -group.
- (iii) H is a class-mate of $(3_+^{1+2})^d$ for some $d \geq 1$.

Our notation is all fairly standard. Let A and B be finite groups and let n and p be positive integers, with p a prime. We denote a cyclic group of order n by C_n (or just n) and A^n is the direct product of n copies of A . In particular, $C_p^n = p^n$ is an elementary abelian p -group of order p^n . If p is an odd prime, then p_+^{1+2m} denotes an extraspecial group of order p^{1+2m} and exponent p , while p_-^{1+2m} has exponent p^2 . A split extension of A by B will be denoted by writing $A:B$, whereas $A.B$ is an unspecified extension. We write $\mathrm{soc}(A)$ for the socle of A (that is, the subgroup of A generated by its minimal normal subgroups). In addition, we adopt the notation from [16] for finite simple groups.

Finally, let us say a few words on the organization of the paper. The next section, which comprises the main bulk of the paper, is dedicated to the proof of Theorem 1, with separate subsections to handle the cases where G is a linear, symplectic, unitary and orthogonal group. A proof of Theorem 2 is presented in Section 3, which includes a detailed analysis of the Type II and III factorizations of almost simple classical groups. Finally, the proof of Theorem 3 is given in Section 4, and Theorems 4 and 5 are established in Section 5.

Acknowledgements. This work was partially supported by NSFC grants 11771200 and 11931005. Burness thanks the Department of Mathematics at the Southern University of Science and Technology (SUSTech) for their generous hospitality during a research visit in April 2019. He also thanks Bob Guralnick for helpful discussions.

2. PROOF OF THEOREM 1

In this section we present a proof of Theorem 1. We will partition the proof into four subsections, according to the socle of the almost simple classical groups we are considering.

Let q be a prime power and let $m \geq 2$ be an integer. Recall that a prime r is a *primitive prime divisor* of $q^m - 1$ if r divides $q^m - 1$, but it does not divide $q^i - 1$ for $1 \leq i < m$. By a theorem of Zsigmondy [30], such a prime always exists, unless $(m, q) = (6, 2)$, or $m = 2$ and q is a Mersenne prime.

2.1. Linear groups. We begin the proof of Theorem 1 by handling Case 1 in Table 1. Recall that a *Singer cycle* in $\mathrm{PGL}_n(q)$ is a cyclic subgroup of order $\frac{q^n - 1}{q - 1}$ (equivalently, it is an irreducible cyclic subgroup of maximal order, with respect to the natural module).

Proposition 2.1. *Let G be an almost simple group with socle $G_0 = \mathrm{PSL}_n(q)$ and subgroups H and K satisfying the conditions in Case 1 of Table 1.*

- (i) *If $G = HK$, then $|H|$ is divisible by $\frac{q^n - 1}{q - 1}$.*

(ii) If $G = \mathrm{PGL}_n(q)$ and $K = P_1$, then $G = HK$ with $H = \frac{q^n-1}{q-1}$ a Singer cycle.

Proof. Here $K \cap G_0 \leq P < G_0$, where P is the stabilizer in G_0 of a 1-dimensional (or $(n-1)$ -dimensional) subspace of the natural module. In particular, $G = HK$ only if $|G_0 : P| = \frac{q^n-1}{q-1}$ divides $|H|$. This establishes part (i). The existence of the factorization in part (ii) follows immediately from the fact that a Singer cycle in $G = \mathrm{PGL}_n(q)$ acts transitively on the set of 1-dimensional subspaces of the natural module for G . \square

Proposition 2.2. *Let G be an almost simple group with socle $G_0 = \mathrm{PSL}_4(q)$ and subgroups H and K satisfying the conditions in Case 2 of Table 1.*

(i) If $G = HK$, then $|H|$ is divisible by $\frac{q^3(q^3-1)}{(2,q-1)}$.

(ii) Let $G \leq \mathrm{PGL}_4(q)$ and $K = \mathrm{PGSp}_4(q) < G$, where

$$G = \begin{cases} \mathrm{PSL}_4(q).2 & \text{if } q \equiv 1 \pmod{4} \\ \mathrm{PSL}_4(q) & \text{otherwise.} \end{cases}$$

Then $G = HK$ with $H = q^3 : \frac{q^3-1}{(2,q-1)} < P_k$ and $k \in \{1, 3\}$.

Proof. Let $P = U:L$ be the stabilizer in G_0 of a 1-dimensional (or 3-dimensional) subspace of the natural module, where U is the unipotent radical and $L = \frac{1}{d}\mathrm{GL}_3(q)$ is a Levi factor, with $d = (4, q-1)$. We may identify U with the natural module for L . According to Table 1 we have

$$H \cap G_0 \leq q^3 : \left(\frac{q^3-1}{d} : 3 \right) < P$$

and we may as well assume K is maximal among subgroups of G with $K \cap G_0 \geq \mathrm{PSp}_4(q)$. Set $e = (2, q-1)$ and note that $\frac{1}{e}q^2(q^3-1)$ divides $|G : K|$.

Suppose $G = HK$, in which case $|H|$ is divisible by $\frac{1}{e}q^2(q^3-1)$ and H contains an element x of order r , a primitive prime divisor of q^3-1 . Then $\langle x \rangle$ acts irreducibly on U and it does not normalize a proper nontrivial subgroup of U . Since $H \cap U \neq 1$, this forces $U \leq H$ and thus $|H|$ is divisible by $\frac{1}{e}q^3(q^3-1)$ as in part (i).

Now let us turn to part (ii). First assume $G = \mathrm{PSL}_4(q)$ with $q \equiv 3 \pmod{4}$ and take $H = q^3 : \frac{q^3-1}{2}$ and $K = \mathrm{PGSp}_4(q)$ (see [16, Proposition 4.8.3]). By arguing as in the proof of [20, Proposition 5.9], noting that the cyclic subgroup of order $\frac{1}{2}(q^3-1)$ acts semiregularly on the set of nonzero vectors in the natural module for L , we deduce that $|H \cap K| = q$ and thus $G = HK$ (here we can appeal to [20, Proposition 5.9] since $G \cong \mathrm{P}\Omega_6^+(q)$). For $q \equiv 1 \pmod{4}$, an entirely similar argument shows that $G = \mathrm{PSL}_4(q).2 < \mathrm{PGL}_4(q)$ admits a factorization $G = HK$ with $H = q^3 : \frac{q^3-1}{2}$ and $K = \mathrm{PGSp}_4(q)$. Finally, the case q even follows directly from [20, Proposition 5.9]. \square

2.2. Symplectic groups. In this section we handle Cases 3, 4 and 5 in Table 1.

Proposition 2.3. *Let G be an almost simple group with socle $G_0 = \mathrm{Sp}_{2m}(q)$, where $m \geq 2$ and q is even. Let H, K be subgroups satisfying the conditions in Case 3 of Table 1.*

(i) If $G = HK$, then $|H|$ is divisible by $q^m(q^m-1)$.

(ii) If $G = \mathrm{Sp}_{2m}(q)$ and $K = \mathrm{O}_{2m}^-(q)$, then $G = HK$ with $H = q^m : (q^m-1) < P_m$.

Proof. Let V be the natural module for G_0 and fix a standard symplectic basis

$$\{e_1, \dots, e_m, f_1, \dots, f_m\}$$

with respect to the underlying symplectic form $(,)$ on V . Let P be the stabilizer in G_0 of the maximal totally isotropic subspace $\langle e_1, \dots, e_m \rangle$ and write $P = U:L$, where the

unipotent radical $U = q^{\frac{1}{2}m(m+1)}$ is elementary abelian and $L = \mathrm{GL}_m(q)$ is a Levi factor. Then

$$H \cap G_0 \leq q^{\frac{1}{2}m(m+1)} : ((q^m - 1) : m) < P$$

and we may assume K is maximal among subgroups of G with $K \cap G_0 = \mathrm{O}_{2m}^-(q)$. Note that $|G : K|$ is divisible by $\frac{1}{2}q^m(q^m - 1)$. The case $G = \mathrm{Sp}_{12}(2)$ can be handled using MAGMA [3], so we may assume $(m, q) \neq (6, 2)$.

Suppose $G = HK$, so $|H|$ is divisible by $\frac{1}{2}q^m(q^m - 1)$. Then H contains an element of order r , a primitive prime divisor of $q^m - 1$, and we note that the smallest nontrivial subgroup of U normalized by $\langle x \rangle$ has order q^m . Therefore, q^m divides $|H|$ and part (i) follows.

Now consider (ii), so $G = \mathrm{Sp}_{2m}(q)$, $K = \mathrm{O}_{2m}^-(q)$ and $H \leq U : ((q^m - 1) : m) < P$. Let X be the natural module for the Levi factor $L = \mathrm{GL}_m(q)$. Now U is indecomposable and reducible as a module for L , with composition series $0 \subseteq W \subseteq U$ where $W = q^{\frac{1}{2}m(m-1)}$. We may identify W and U/W with the modules $\Lambda^2(X)$ and X , respectively.

Let $C = \langle c \rangle < L$ be a Singer cycle and write $U = W \oplus W'$, where W' is an irreducible m -dimensional module for C , which we can, and will, identify with X .

Claim. *We have $G = HK$ with $H = X : C = q^m : (q^m - 1)$.*

By the proof of [20, Proposition 5.5] we have $H \cap K = X \cap K$, so $|X \cap K| \geq 2$. Since C acts transitively on the set of nontrivial elements in X , we may write

$$X = \{1\} \cup z^C$$

for some $z \in K$. With respect to an appropriate basis for V , we have

$$z = \begin{pmatrix} I_m & A \\ 0 & I_m \end{pmatrix} \quad (1)$$

for a matrix A of size m . Moreover, if $s = \mathrm{rank}(A)$ then z has Jordan form $[J_2^s, J_1^{2m-2s}]$ on V , where J_i denotes a standard unipotent Jordan block of size i .

The conjugacy classes of involutions in G are described by Aschbacher and Seitz in [1]. In their notation, which is now standard, every involution in G is of type a , b or c , and the a -type involutions x are characterised by the property $(v, v^x) = 0$ for all $v \in V$. From the description of the elements in $(U \cap K) \setminus W$ given in the proof of [20, Proposition 5.5], it is routine to check that there exists a vector $v \in V$ such that $(v, v^z) \neq 0$, whence z is G -conjugate to b_s (if s is odd) or c_s (if s is even).

Set $N = N_L(C) = C : D$, where $D = \langle \varphi \rangle$ has order m , and let $\bar{X} = X \otimes \mathbb{F}_{q^m}$. Fix a basis $\{x_1, \dots, x_m\}$ for \bar{X} such that $x_i^c = \mu^{q^i-1} x_i$ for $i = 1, \dots, m$, where $\mathbb{F}_{q^m}^\times = \langle \mu \rangle$. We may assume that φ cyclically permutes the x_i .

Observe that D has a 1-dimensional fixed space on both X and \bar{X} . Since $\langle u \rangle$ is the fixed space of D on \bar{X} , where $u = x_1 + \dots + x_m$, it follows that some nonzero \mathbb{F}_{q^m} -scalar multiple of u is contained in X . Without loss of generality, we may assume that u itself is in X (the calculation below does not depend on the choice of scalar multiple). This means that X is generated by u (as a module for C) and we deduce that

$$X = \{\alpha x_1 + \alpha^q x_2 + \dots + \alpha^{q^{m-1}} x_m : \alpha \in \mathbb{F}_{q^m}\}.$$

In terms of the basis $\{x_1, \dots, x_m\}$ for \bar{X} , each nontrivial element of X is represented by a nonsingular diagonal matrix. This implies that the matrix A in (1) has rank m and we conclude that all of the involutions in X are of type b_m (if m is odd) or c_m (if m is even).

To complete the proof of the claim, let n denote the number of orbits of H on $\Delta = G/K$. By the orbit counting lemma, we have

$$n = \frac{1}{|H|} \sum_{h \in H} \text{fix}(h),$$

where $\text{fix}(h)$ is the number of fixed points of h on Δ . Since $H \cap K = X \cap K$, it follows that $\text{fix}(h) = 0$ for all $h \in H \setminus X$ and thus

$$n = \frac{1}{|H|} \sum_{x \in X} \text{fix}(x) = \frac{1}{|H|} (|\Delta| + |z^C| \cdot \text{fix}(z)).$$

From the description of the conjugacy classes of involutions in K and G given in [1] we deduce that $z^G \cap K = z^K$ and thus

$$\text{fix}(z) = |\Delta| \cdot \frac{|z^G \cap K|}{|z^G|} = \frac{|C_G(z)|}{|C_K(z)|}.$$

By reading off the relevant centralizer orders (see [5, Tables 3.4.1, 3.5.1], for example) we calculate that $\text{fix}(z) = \frac{1}{2}q^m$ and thus $n = 1$. In other words, $G = HK$ as required. \square

Remark 2.4. The existence of a factorization $G = HK$ in this case with $H = q^m:(q^m - 1)$ was first established by Guralnick and Saxl in the proof of [8, Theorem 3.1] (see p.139 and the first case considered in Step 7 of the proof). They proceed as follows. First let $J = \text{Sp}_2(q^m) < G$. Then by arguing as in [21] (see Case 3.2.1(d) on p.48) we deduce that $G = JK$ and $J \cap K = \text{O}_2^-(q^m)$. Therefore, if $H = q^m:(q^m - 1)$ is the Borel subgroup of J , then we must have $|H \cap K| = 2$ since $(|J \cap K|, |H|) = 2$, and we conclude that $G = HK$.

Proposition 2.5. *Let G be an almost simple group with socle $G_0 = \text{Sp}_4(q)$, where q is even, and let H, K be subgroups satisfying the conditions in Case 4 of Table 1.*

- (i) *If $G = HK$, then $|H|$ is divisible by $q^2(q^2 - 1)$.*
- (ii) *If $G = \text{Sp}_4(q)$ and $K = \text{Sp}_2(q^2).2$, then $G = HK$ with $H = q^2:(q^2 - 1) < P_1$.*

Proof. By applying a graph automorphism of G_0 , we may view Case 4 in Table 1 as a special version of Case 3 (with $m = 2$) and so the result follows from Proposition 2.3. \square

Proposition 2.6. *Let G be an almost simple group with socle $G_0 = \text{PSp}_4(q)$, where q is odd, and let H, K be subgroups satisfying the conditions in Case 5 of Table 1.*

- (i) *If $G = HK$ then $|H|$ is divisible by $q^3(q^2 - 1)$.*
- (ii) *If $G = \text{PGSp}_4(q)$ and $K = \text{PGSp}_2(q^2).2$, then $G = HK$ with $H = q^{1+2}:(q^2 - 1)$ contained in P_1 .*

Proof. In view of the isomorphism $\text{PSP}_4(q) \cong \Omega_5(q)$, we can consider Case 5 in Table 1 as a special version of Case 7 (with $m = 2$). Our analysis of Case 7 in Proposition 2.8 below includes the case $m = 2$, and the result for Case 5 follows immediately. \square

2.3. Unitary groups.

Proposition 2.7. *Let G be an almost simple group with socle $G_0 = \text{PSU}_{2m}(q)$, where $m \geq 2$, and let H and K be subgroups satisfying the conditions in Case 6 of Table 1.*

- (i) *If $G = HK$, then $|H|$ is divisible by $\frac{q^{2m}(q^{2m}-1)}{q+1}$.*
- (ii) *If $G = \text{PGU}_{2m}(q)$ and $K = N_1$, then $G = HK$ with $H = q^{2m}:\frac{q^{2m}-1}{q+1} < P_m$.*

Proof. Let V be the natural module for G_0 and fix a standard basis $\{e_1, \dots, e_m, f_1, \dots, f_m\}$ with respect to the defining unitary form on V . We have

$$H \cap G_0 \leq q^{m^2} : \left(\frac{q^{2m} - 1}{(q+1)d} \cdot m \right) < P,$$

where $d = (2m, q+1)$ and P is the stabilizer in G_0 of the totally isotropic space $\langle e_1, \dots, e_m \rangle$. Here q^{m^2} is the unipotent radical of P , which is elementary abelian. We may assume that K is the stabilizer in G of a nondegenerate 1-space, so K is a maximal subgroup of type $\mathrm{GU}_{2m-1}(q) \times \mathrm{GU}_1(q)$ and

$$|G : K| = q^{2m-1} \frac{q^{2m} - 1}{q+1}.$$

The case $(m, q) = (3, 2)$ can be handled using MAGMA, so we may assume $(m, q) \neq (3, 2)$.

Suppose $G = HK$. Then $|H|$ is divisible by $q^{2m-1} \frac{q^{2m}-1}{q+1}$ and thus H contains an element x of order r , a primitive prime divisor of $q^{2m} - 1$. By considering the action of $\langle x \rangle$ on the unipotent radical of P we deduce that q^{2m} divides $|H|$ and part (i) follows.

Now let us turn to part (ii). If $m = 2$ then $m^2 = 2m$ and the existence of the factorization in (ii) follows immediately from [20, Proposition 5.2]. For the remainder let us assume $m \geq 3$.

It will be convenient to work in the matrix group $G = \mathrm{GU}_{2m}(q)$, so we take $K = \mathrm{GU}_{2m-1}(q) \times \mathrm{GU}_1(q)$ and we consider a subgroup

$$H \leq q^{m^2} : ((q^{2m} - 1) : m) < q^{m^2} : \mathrm{GL}_m(q^2) = U : L = P,$$

where $U = q^{m^2}$ and $L = \mathrm{GL}_m(q^2)$ (once again, P denotes the stabilizer in G of $\langle e_1, \dots, e_m \rangle$). Our goal is to construct a subgroup $H = q^{2m} : (q^{2m} - 1)$ with $G = HK$, so that by passing to the quotient group $G/Z(G)$, we obtain a factorization of $\mathrm{PGU}_{2m}(q)$ of the required form.

Let $C = \langle c \rangle = C_{q^{2m}-1}$ be a Singer cycle in L and let W be a $(2m)$ -dimensional irreducible summand for the action of C on U . Let $N = N_L(C) = C : D$, where $D = \langle \varphi \rangle$ has order m . Set $H = W : C < P$.

Claim. *We have $G = HK$.*

Let X be the natural module for L and let $\sigma : L \rightarrow L$ be the involutory automorphism induced by the action of the field automorphism $\lambda \mapsto \lambda^q$ on matrix entries. If X affords the representation $\rho : L \rightarrow \mathrm{GL}_m(q^2)$, then we write $X^{(q)}$ for the space X with L -action given by the representation $\sigma\rho$.

Consider the module $X \otimes X^{(q)}$ for L , which has dimension m^2 as a space over \mathbb{F}_{q^2} . This module is defined over \mathbb{F}_q (see [4, Theorem 5.1.13], for example) and we can identify U with the \mathbb{F}_q -span of a suitable basis for $X \otimes X^{(q)}$. In terms of the above standard basis for V , each $u \in U$ can be expressed as a matrix of the form

$$u = \begin{pmatrix} I_m & A \\ 0 & I_m \end{pmatrix} \tag{2}$$

for some matrix A of size m and it follows that u has Jordan form $[J_2^s, J_1^{2m-2s}]$ on the natural module for G , where $s = \mathrm{rank}(A)$.

Now extend scalars and set $\bar{X} = X \otimes \mathbb{F}_{q^{2m}}$ and $\bar{U} = U \otimes \mathbb{F}_{q^{2m}}$, so we have

$$U \subseteq X \otimes X^{(q)} \subseteq \bar{X} \otimes \bar{X}^{(q)} = \bar{U}.$$

Fix a basis $\{x_1, \dots, x_m\}$ for \bar{X} comprising eigenvectors for c (a generator for the Singer cycle $C < L$), say $x_i^c = \mu^{q^{2(i-1)}} x_i$ for each i , where $\mathbb{F}_{q^{2m}}^\times = \langle \mu \rangle$. We may assume that φ

cyclically permutes the x_i , sending x_1 to x_2 , etc. Then

$$\{x_i \otimes x_j : 1 \leq i, j \leq m\}$$

is a basis for \bar{U} . In particular, if $u \in U$ and we write $u = \sum_{i,j} b_{ij}(x_i \otimes x_j)$ and $B = (b_{ij})$, then the rank of B coincides with the rank of A in (2).

Set $J = \text{GL}_m(q^2).2 = L.2 \leq \Gamma\text{L}_m(q^2)$ and observe that we may view U and \bar{U} as modules for J . Set $M = N_J(C) = C:E$, where $E = \langle \sigma \rangle$ has order $2m$ and $\sigma^2 = \varphi$. Without loss of generality, we may assume that σ sends $x_i \otimes x_j$ to $x_{j+1} \otimes x_i$ for all i, j (reading subscripts mod m).

Consider $\bar{W} = W \otimes \mathbb{F}_{q^{2m}}$ as a subspace of \bar{U} . Now W is absolutely irreducible as a module for M , so \bar{W} is irreducible for M . It is straightforward to decompose \bar{U} as a sum of irreducible M -modules. For convenience of notation, let us assume that \bar{W} is the submodule generated by $x_1 \otimes x_3$, so

$$\bar{W} = \langle x_1 \otimes x_3, x_4 \otimes x_1, x_2 \otimes x_4, \dots, x_3 \otimes x_m \rangle$$

(reading subscripts mod m). Now σ has a 1-dimensional fixed space on both W and \bar{W} . On the latter space, this is clearly $\langle w \rangle$, where

$$w = x_1 \otimes x_3 + x_4 \otimes x_1 + x_2 \otimes x_4 + \dots + x_3 \otimes x_m.$$

We may assume that w is contained in W (the computations below do not change if w is replaced by a scalar multiple), which implies that

$$W = \{ \alpha(x_1 \otimes x_3) + \alpha^q(x_4 \otimes x_1) + \alpha^{q^2}(x_2 \otimes x_4) + \dots + \alpha^{q^{2m-1}}(x_3 \otimes x_m) : \alpha \in \mathbb{F}_{q^{2m}} \}.$$

Suppose

$$v = \alpha(x_1 \otimes x_3) + \alpha^q(x_4 \otimes x_1) + \alpha^{q^2}(x_2 \otimes x_4) + \dots + \alpha^{q^{2m-1}}(x_3 \otimes x_m) = \sum_{i,j} b_{ij}(x_i \otimes x_j)$$

is a nontrivial element of W and set $B = (b_{ij})$ and $\ell = \frac{q^{2m}-1}{q+1}$. Then it is straightforward to check that

$$\text{rank}(B) = \begin{cases} m-1 & \text{if } \alpha^\ell = (-1)^m \\ m & \text{otherwise} \end{cases}$$

and thus W contains ℓ elements with Jordan form $[J_2^{m-1}, J_1^2]$ and the remaining nontrivial elements have Jordan form $[J_2^m]$.

Let $\Delta = G/K$ and let n be the number of orbits of H on Δ . Note that we may identify Δ with the set of 1-dimensional nondegenerate subspaces of the natural module for G . Also observe that $Z(G) = C_{q+1}$ is the kernel of the action.

Since $H \cap K = (W \cap K) \times Z(G)$ and elements of type $[J_2^m]$ have no fixed points on Δ , it follows that

$$n = \frac{1}{|H|} \sum_{h \in H} \text{fix}(h) = \frac{1}{|H|} ((q+1)|\Delta| + \ell(q+1) \cdot \text{fix}(z)),$$

where $z \in W \cap K$ has Jordan form $[J_2^{m-1}, J_1^2]$. Now $z^G \cap K = z^K$ and we calculate that

$$\text{fix}(z) = \frac{|C_G(z)|}{|C_K(z)|} = q^{2m-1}(q-1).$$

It is now routine to check that this gives $n = 1$ and thus $G = HK$. \square

2.4. Orthogonal groups. We are now ready to complete the proof of Theorem 1 by handling Cases 7, 8 and 9 in Table 1.

First we consider Case 7. In the statement of the following proposition, it is convenient to allow the case $m = 2$, which is excluded in Table 1 (cf. Proposition 2.6). In part (ii), we use N_1^- to denote the stabilizer in $\mathrm{SO}_{2m+1}(q)$ of a nondegenerate 1-space W such that W^\perp is a minus-type orthogonal space.

Proposition 2.8. *Let G be an almost simple group with socle $G_0 = \Omega_{2m+1}(q)$, where $m \geq 2$ and q is odd. Let H, K be subgroups satisfying the conditions in Case 7 of Table 1.*

(i) *If $G = HK$, then $|H|$ is divisible by $\frac{1}{e}q^{\frac{1}{2}m(m+1)}(q^m - 1)$, where*

$$e = \begin{cases} 2 & \text{if } q^m \equiv 3 \pmod{4} \\ 1 & \text{otherwise.} \end{cases}$$

(ii) *If $G = \mathrm{SO}_{2m+1}(q)$ and $K = N_1^-$, then $G = HK$ with*

$$H = (q^{\frac{1}{2}m(m-1)}.q^m) : \frac{q^m - 1}{e} < P_m.$$

Proof. Let V be the natural module for G_0 and fix a standard basis

$$\{e_1, \dots, e_m, f_1, \dots, f_m, v\}.$$

Let P be the stabilizer in G_0 of the maximal totally singular subspace $\langle e_1, \dots, e_m \rangle$ and write $P = U:L$, where the unipotent radical U is nonabelian of order $q^{\frac{1}{2}m(m+1)}$ and $L = \frac{1}{2}\mathrm{GL}_m(q)$ is a Levi factor. Here $Z(U) = q^{\frac{1}{2}m(m-1)}$ is the unique minimal normal subgroup of P and we may identify $U/Z(U)$ with the natural module for $\mathrm{GL}_m(q)$. Write $q = p^f$, where p is a prime.

Now

$$H \cap G_0 \leq (q^{\frac{1}{2}m(m-1)}.q^m) : \left(\frac{q^m - 1}{2}.m \right) < P$$

and we may assume that K is the stabilizer in G of the 1-space $\langle e_m + \mu f_m \rangle$, where $\mu \in \mathbb{F}_q$ is a non-square. In other words, K is a maximal subgroup of G of type $\mathrm{O}_{2m}^-(q)$ and we note that $|G : K| = \frac{1}{2}q^m(q^m - 1)$.

As in the proof of [20, Proposition 5.5], define the following linear maps on V for $1 \leq i < j \leq m$ and $\lambda \in \mathbb{F}_q$, where

$$y_{i,j}(\lambda) : f_i \mapsto f_i + \lambda e_j, \quad f_j \mapsto f_j - \lambda e_i$$

and $y_{i,j}(\lambda)$ fixes the remaining basis elements. It is straightforward to check that each $y_{i,j}(\lambda)$ is contained in $Z(U)$. Therefore, since $|Z(U)| = q^{\frac{1}{2}m(m-1)}$, we conclude that

$$Z(U) = \langle y_{i,j}(\lambda) : 1 \leq i < j \leq m, \lambda \in \mathbb{F}_q \rangle$$

and thus

$$Z(U) \cap K = \langle y_{i,j}(\lambda) : 1 \leq i < j < m, \lambda \in \mathbb{F}_q \rangle$$

is elementary abelian of order $q^{\frac{1}{2}(m-1)(m-2)}$.

Claim. *We have $G = HK$ only if $U \leq H$.*

Seeking a contradiction, suppose $G = HK$ and $W = H \cap U < U$. Notice that if $\mathrm{SO}_{2m+1}(q) \not\leq G$, then by taking $G_1 = \langle \mathrm{SO}_{2m+1}(q), G \rangle$ we can construct a factorization $G_1 = HK_1$ with $K_1 = N_{G_1}(K)$. Therefore, without loss of generality, we may assume that G contains $\mathrm{SO}_{2m+1}(q)$, so $G = \mathrm{SO}_{2m+1}(q).f'$ for some divisor f' of f .

First assume $W = Z(U)$. Then without loss of generality, we may assume that $H = W:(C.m.f')$, where $C < \text{GL}_m(q)$ is a Singer cycle. Since $Z(U) \cap K \leq H \cap K$, it follows that $q^{\frac{1}{2}(m-1)(m-2)}$ divides

$$|H \cap K| = \frac{|H||K|}{|G|} = 2mf'q^{\frac{1}{2}m(m-3)}$$

and thus q divides $2mf'$. Let $J = W:C$, which is a normal subgroup of H of index mf' . Then $J \cap K$ is normal in $H \cap K$ and the proof of [20, Proposition 5.5] implies that $J \cap K = W \cap K$. Therefore, we can write

$$H \cap K = (J \cap K).R,$$

where $R \leq C.m.f'$ has order $\frac{2mf'}{q}$. Since $|R \cap C| = 1$, we have

$$R \cong RC/C \leq (C.m.f')/C \cong C_m.C_{f'}$$

and thus $|R| = \frac{2mf'}{q}$ divides mf' . But this is absurd since q is odd.

Next suppose $W < Z(U)$. Then $G = \tilde{H}K$, where $\tilde{H} = Z(U)H$ and $\tilde{H} \cap U = Z(U)$. But we have just ruled out the existence of such a factorization, so the case $W < Z(U)$ does not arise.

To complete the proof of the claim, we may assume $W \cap Z(U) < W$, in which case $WZ(U)/Z(U) \leq U/Z(U)$ is nontrivial. Write $H = W:D$, where $|D|$ is divisible by $\frac{q^m-1}{2}$, and note that

$$HZ(U)/Z(U) = (WZ(U)/Z(U)):D \leq (U/Z(U)):D.$$

Suppose $q^m - 1$ is divisible by a primitive prime divisor r . Then D contains an element x of order r and $\langle x \rangle$ does not normalize a proper nontrivial subgroup of $U/Z(U)$. Therefore, $WZ(U)/Z(U) = U/Z(U)$ and thus $WZ(U) = U$. In particular, $W \cap Z(U)$ is a normal subgroup of U . If $W \cap Z(U) = 1$ then $W \cong U/Z(U)$ is abelian and thus $U \cong W \times Z(U)$ is abelian, which is a contradiction. Therefore, $W \cap Z(U)$ is a nontrivial normal subgroup of U , so it must contain $Z(U)$, which is the unique minimal normal subgroup of U . It follows that $Z(U) \leq W \cap Z(U)$, so $W = U$ and once again we have reached a contradiction.

Finally, let us assume $q^m - 1$ does not have a primitive prime divisor, so Zsigmondy's theorem [30] implies that $m = 2$ and q is a Mersenne prime. In particular, $G = \text{SO}_5(q)$, $|U| = q^3$, $|Z(U)| = q$ and $|W| = q^2$ (recall that $|H|$ is divisible by $|G : K| = \frac{1}{2}q^2(q^2 - 1)$). Let us also note that $D \leq (q^2 - 1):2$. The case $q = 3$ can be handled directly using MAGMA [3], so we may assume $q \geq 7$. Then D contains an element x of order $\frac{q^2-1}{4}$ and $\langle x \rangle$ does not normalize a proper nontrivial subgroup of $U/Z(U)$. Therefore, $WZ(U)/Z(U) = U/Z(U)$ and we reach a contradiction by repeating the argument in the previous paragraph.

With the claim in hand, let G be an arbitrary almost simple group with socle G_0 and a factorization $G = HK$. Since $U \leq H$ and $\frac{1}{2}q^m(q^m - 1)$ divides $|H|$, it follows that $|H|$ is divisible by $\frac{1}{2}q^{\frac{1}{2}m(m+1)}(q^m - 1)$.

Suppose $|H| = \frac{1}{2}q^{\frac{1}{2}m(m+1)}(q^m - 1)$. As before, without loss of generality we can assume that $G = \text{SO}_{2m+1}(q).f'$, where f' divides f . Then we may write

$$H = U: \left(\frac{q^m - 1}{2ab}.a \right).b,$$

where a divides m and b divides f' . Let $C < \text{GL}_m(q)$ be a Singer cycle and let D be the unique index-two subgroup of C .

First assume $a = b = 1$, so $H = U:D$ and we define $J = U:C$. Then [20, Proposition 5.7] implies that $G = JK$, so J acts transitively on $\Delta = G/K$. In turn, U acts $\frac{1}{2}$ -transitively on Δ (that is, all the orbits of U have the same size, namely q^m) and the orbits of U form

a block system \mathcal{B} for the action of J , with $|\mathcal{B}| = \frac{1}{2}(q^m - 1)$. Now $J/U \cong C$ is transitive on \mathcal{B} and thus the unique involution $z \in C$ is in the kernel of this action. It follows that D acts transitively on \mathcal{B} , whence $G = HK$ if and only if $z \notin D$. That is, $G = HK$ if and only if $|D|$ is odd, which is equivalent to the condition $q^m \equiv 3 \pmod{4}$.

Now assume $(a, b) \neq (1, 1)$ and write $H = U:E$, where $E = \left(\frac{q^m-1}{2ab}.a\right).b$. As above, the orbits of U on $\Delta = G/K$ form a block system \mathcal{B} with $|\mathcal{B}| = \frac{1}{2}(q^m - 1)$. Since C acts transitively on \mathcal{B} , it follows that the unique involution in C is contained in the kernel of this action.

Claim. *If $q^m \equiv 1 \pmod{4}$, then $\frac{q^m-1}{2ab}$ is even.*

Write $fm = 2^k \ell$ with ℓ odd and set $r = p^\ell$. Then $q^m = p^{fm} = r^{2^k}$. Since a divides m and b divides f , the 2-part of ab divides 2^k , which is the 2-part of fm . Factorize $q^m - 1$ as follows

$$q^m - 1 = r^{2^k} - 1 = (r^{2^{k-1}} + 1)(r^{2^{k-2}} + 1) \cdots (r + 1)(r - 1).$$

Since each factor $r^{2^i} + 1$ is even and $(r + 1)(r - 1)$ is divisible by 8, we conclude that $q^m - 1$ is divisible by $4ab$ and so $\frac{q^m-1}{2ab}$ is even as claimed.

It follows that if $q^m \equiv 1 \pmod{4}$ then E contains the involution in C and thus E is intransitive on \mathcal{B} . In particular, $G \neq HK$. An entirely similar argument shows that if $q^m \equiv 1 \pmod{4}$ then $|H|$ is divisible by $q^{\frac{1}{2}m(m+1)}(q^m - 1)$ and we have now established part (i).

Finally, let us turn to part (ii), so $G = \text{SO}_{2m+1}(q)$. If $q \equiv 1 \pmod{4}$ then the result follows immediately from [20, Proposition 5.7]. Similarly, if $q^m \equiv 3 \pmod{4}$ then the above argument (the case $a = b = 1$) shows that $G = HK$ with $H = U:D$ and $K = N_1^-$. This completes the proof of the proposition. \square

Next we handle Case 8 in Table 1. Note that we include the case $m = 4$, so this also covers Case 9 in Table 1. In particular, the following proposition completes the proof of Theorem 1. In part (iii), N_1 denotes the stabilizer of a nondegenerate 1-space.

Proposition 2.9. *Let G be an almost simple group with socle $G_0 = \text{P}\Omega_{2m}^+(q)$, where $m \geq 4$, and let H and K be subgroups satisfying the conditions in Case 8 of Table 1.*

- (i) *If $G = HK$, then $|H|$ is divisible by $\frac{q^m(q^m-1)}{(2, q-1)}$.*
- (ii) *If q is even, $G = \Omega_{2m}^+(q)$ and $K = \text{Sp}_{2m-2}(q)$, then $G = HK$ with $H = q^m:(q^m-1)$.*
- (iii) *If q is odd, $G = \text{PSO}_{2m}^+(q)$ and $K = N_1$, then $G = HK$ with $H = q^m:\frac{q^m-1}{2}$.*

In parts (ii) and (iii), the given subgroup H is contained in P_m .

Proof. To begin with, let us assume q is even. Let V be the natural module for G_0 and fix a standard basis $\mathcal{B} = \{e_1, \dots, e_m, f_1, \dots, f_m\}$. Let $P = U:L$ be the stabilizer in G_0 of the totally singular subspace $\langle e_1, \dots, e_m \rangle$, where the unipotent radical U is elementary abelian of order $q^{\frac{1}{2}m(m-1)}$ and $L = \text{GL}_m(q)$ is a Levi factor. Then

$$H \cap G_0 \leq q^{\frac{1}{2}m(m-1)}:((q^m - 1):m) < P$$

and we may assume that K is maximal among subgroups of G with $K \cap G_0 = \text{Sp}_{2m-2}(q)$. Note that $|G : K|$ is divisible by $q^{m-1}(q^m - 1)$. We can use MAGMA to handle the case $G_0 = \Omega_{12}^+(2)$, so we may assume $(m, q) \neq (6, 2)$.

If $G = HK$ then $|H|$ is divisible by $q^{m-1}(q^m - 1)$ and by repeating the argument in the proof of Proposition 2.3, we deduce that $q^m(q^m - 1)$ divides $|H|$. This gives part (i).

Next let us turn to (ii). Set $G = \Omega_{2m}^+(q)$. Let $C = \langle c \rangle$ be a Singer cycle in L and set $N = N_L(C) = C:D$, where $D = \langle \varphi \rangle$ has order m . As a module for L , we may identify U with $\Lambda^2(X)$, where X is the natural module for L . In terms of the basis \mathcal{B} , we can express each $u \in U$ as in (2) for some matrix A of size m and we see that u has Jordan form $[J_2^s, J_1^{2m-2s}]$ on V , where $s = \text{rank}(A)$. Moreover, one checks that every nontrivial element in U is an involution of type a (with respect to [1]), so u is G -conjugate to a_s .

Write $\bar{X} = X \otimes \mathbb{F}_{q^m}$ and $\bar{U} = \Lambda^2(\bar{X})$. The action of c on \bar{X} is diagonalizable and we may choose a basis $\{x_1, \dots, x_m\}$ for \bar{X} such that $x_i^c = \mu^{q^{i-1}} x_i$ for $i = 1, \dots, m$, where $\mathbb{F}_{q^m}^\times = \langle \mu \rangle$. Then

$$\{x_i \wedge x_j : 1 \leq i < j \leq m\}$$

is a basis for \bar{U} and we may assume that φ cyclically permutes the x_i . In particular, if $u \in U$ and we write $u = \sum_{i,j} b_{ij}(x_i \wedge x_j)$, then the corresponding alternating matrix $B = (b_{ij})$ of size m has the same rank as the matrix A in (2). Therefore, the rank of B determines the G -class of u .

Consider the action of C on U and let W be an irreducible submodule of dimension m . Then W is absolutely irreducible as a module for N and thus $\bar{W} = W \otimes \mathbb{F}_{q^m}$ is an irreducible N -module. It is straightforward to decompose \bar{U} as a direct sum of irreducible modules for N and we may assume that W has been chosen so that

$$\bar{W} = \langle x_1 \wedge x_2, x_2 \wedge x_3, \dots, x_m \wedge x_1 \rangle.$$

Set

$$w = x_1 \wedge x_2 + x_2 \wedge x_3 + \dots + x_{m-1} \wedge x_m + x_m \wedge x_1 \in \bar{W}$$

and $H = W:C = q^m:(q^m - 1)$.

Claim. *We have $G = HK$.*

To see this, observe that $\varphi \in N$ has a 1-dimensional fixed space on both W and \bar{W} . Clearly, $\langle w \rangle$ is the fixed point space of φ on \bar{W} , so W must contain a nonzero scalar multiple of w . Without loss of generality, we may assume that $w \in W$, so W is generated by w as a C -module and we deduce that

$$W = \{\alpha(x_1 \wedge x_2) + \alpha^q(x_2 \wedge x_3) + \dots + \alpha^{q^{m-2}}(x_{m-1} \wedge x_m) + \alpha^{q^{m-1}}(x_m \wedge x_1) : \alpha \in \mathbb{F}_{q^m}\}.$$

If m is odd and $z \in W$ is nontrivial, then a straightforward calculation shows that $\text{rank}(z) = m - 1$ and thus z is an involution in G of type a_{m-1} . By applying the orbit counting lemma with respect to the action of H on $\Delta = G/K$, noting that we have $|\Delta| = q^{m-1}(q^m - 1)$ and $\text{fix}(h) = 0$ for all $h \in H \setminus W$ (see the proof of [20, Proposition 5.9]), we calculate that H has

$$n = \frac{1}{|H|} (|\Delta| + (q^m - 1) \cdot \text{fix}(z))$$

orbits on Δ . Now $z^G \cap K = z^K$ and we deduce that

$$\text{fix}(z) = \frac{|C_G(z)|}{|C_K(z)|} = q^{m-1}(q - 1),$$

which yields $n = 1$. Therefore, $G = HK$ as claimed.

Now assume m is even and fix a nontrivial element

$$z = \alpha(x_1 \wedge x_2) + \alpha^q(x_2 \wedge x_3) + \dots + \alpha^{q^{m-2}}(x_{m-1} \wedge x_m) + \alpha^{q^{m-1}}(x_m \wedge x_1) \in W.$$

Set $\ell = \frac{q^m - 1}{q + 1}$. A calculation shows that

$$\text{rank}(z) = \begin{cases} m - 2 & \text{if } \alpha^\ell = 1 \\ m & \text{otherwise.} \end{cases}$$

Therefore, W contains ℓ involutions of type a_{m-2} , and the remaining involutions in W are of type a_m . Since the latter involutions have no fixed points on $\Delta = G/K$, it follows that H has

$$n = \frac{1}{|H|} (|\Delta| + \ell \cdot \text{fix}(z))$$

orbits on Δ , where z is an involution of type a_{m-2} . It is straightforward to check that

$$\text{fix}(z) = \frac{|C_G(z)|}{|C_K(z)|} = q^{m-1}(q^2 - 1)$$

and this gives $n = 1$ as required.

To complete the proof of the proposition, let us assume q is odd. Here we take K to be maximal among subgroups of G with $K \cap G_0 \supseteq \Omega_{2m-1}(q)$, so $|G : K|$ is divisible by $\frac{1}{2}q^{m-1}(q^m - 1)$. In particular, if $G = HK$ then $|H|$ is divisible by $\frac{1}{2}q^{m-1}(q^m - 1)$ and by considering an element of order r , a primitive prime divisor of $q^m - 1$, we quickly deduce that q^m divides $|H|$. Therefore, $\frac{1}{2}q^m(q^m - 1)$ divides $|H|$ as in part (i).

Finally, let us turn to part (iii). Here it will be convenient to work in the matrix group $G = \text{SO}_{2m}^+(q)$ and we will establish the existence of a factorization $G = HK$ with $H = q^m : (q^m - 1)$. Then by taking quotients, we will obtain the desired factorization of $G/Z(G) = \text{PSO}_{2m}^+(q)$.

As before, let $\{e_1, \dots, e_m, f_1, \dots, f_m\}$ be a standard basis for the natural module V and let $P = U:L$ be the stabilizer in G of the subspace $\langle e_1, \dots, e_m \rangle$, where U is elementary abelian of order $q^{\frac{1}{2}m(m-1)}$ and $L = \text{GL}_m(q)$. Each $u \in U$ can be expressed as a matrix as in (2) and we deduce that u has Jordan form $[J_2^s, J_1^{2m-2s}]$ on V , where $s = \text{rank}(A)$. Let $C = \langle c \rangle < L$ be a Singer cycle and let $W \subseteq U$ be an irreducible summand of dimension m with respect to the action of C on U .

Let $H = W:C = q^m : (q^m - 1)$ and let $\Delta = G/K$, where $K = \text{SO}_{2m-1}(q) \times C_2$ is the stabilizer of a nondegenerate 1-space. We claim that $G = HK$. As before, we will use the orbit counting lemma to show that $n = 1$, where n is the number of orbits of H on Δ . Note that $Z(G) = C_2$ is the kernel of the action, which contains the element of order 2 in C . By the proof of [20, Proposition 5.9], we have $H \cap K = (W \cap K) \times Z(G)$.

First assume m is odd. By repeating the argument in the q even case, we deduce that every nontrivial element in W has Jordan form $[J_2^{m-1}, J_1^2]$. Now G has a unique conjugacy class of such elements and thus

$$n = \frac{1}{|H|} \sum_{h \in H} \text{fix}(h) = \frac{1}{|H|} (2|\Delta| + 2(q^m - 1) \cdot \text{fix}(z)),$$

where $z \in W \cap K$ is nontrivial. Since $\text{SO}_{2m-1}(q)$ has a unique class of unipotent elements with Jordan form $[J_2^{m-1}, J_1]$, we deduce that $z^G \cap K = z^K$ and so we get

$$\text{fix}(z) = |\Delta| \cdot \frac{|z^G \cap K|}{|z^G|} = \frac{|C_G(z)|}{|C_K(z)|}.$$

By reading off the relevant centralizer orders (see [5, Section 3.5.3]), we deduce that

$$|C_G(z)| = q^{\frac{1}{2}m^2 + \frac{1}{2}m-1} |\text{Sp}_{m-1}(q)| |\text{SO}_2^+(q)|, \quad |C_K(z)| = 2q^{\frac{1}{2}m^2 - \frac{1}{2}m} |\text{Sp}_{m-1}(q)|$$

and thus

$$\text{fix}(z) = \frac{1}{2} q^{m-1} (q - 1).$$

One now checks that this gives $n = 1$, as required.

A similar argument applies when m is even. Proceeding as in the q even case, we deduce that $\ell = \frac{q^m - 1}{q + 1}$ elements in W have Jordan form $[J_2^{m-2}, J_1^4]$ on V , and the remaining nontrivial elements have Jordan form $[J_2^m]$. Since none of the latter elements fix a

nondegenerate 1-space, it follows that

$$n = \frac{1}{|H|} \sum_{h \in H} \text{fix}(h) = \frac{1}{|H|} (2|\Delta| + 2\ell \cdot \text{fix}(z)),$$

where $z \in W \cap K$ is nontrivial. As above, we have $z^G \cap K = z^K$ and we calculate that

$$\text{fix}(z) = \frac{|C_G(z)|}{|C_K(z)|} = \frac{1}{2}q^{m-1}(q^2 - 1).$$

This gives $n = 1$ and the proof of the proposition is complete. \square

This completes the proof of Theorem 1.

3. PROOF OF THEOREM 2

In this section we prove Theorem 2, which gives the minimal order $\ell(G_0)$ of a solvable factor of any almost simple group G with socle G_0 .

Proposition 3.1. *The conclusion to Theorem 2 holds if G_0 is non-classical.*

Proof. As noted in Section 1, we have $\ell(G_0) = 0$ if G_0 is an exceptional group of Lie type. If $G_0 = A_n$ then every core-free subgroup of G has index at least n , so every solvable factor has order at least n . But if $G = S_n$ and $H = \langle g \rangle$ with g an n -cycle, then $G = HK$ with $K = S_{n-1}$, whence $\ell(G_0) = n$. Finally, if G_0 is a sporadic group then the relevant factorizations are recorded in [20, Proposition 4.4] and we can read off $\ell(G_0)$. \square

To complete the proof of Theorem 2, we need to handle the factorizations $G = HK$ of almost simple classical groups. Recall from Section 1 that such a factorization is of Type I, II or III, according to the following definition:

- I. $(G_0, H \cap G_0, K \cap G_0)$ belongs to one of 9 infinite families listed in [20, Table 1.1];
- II. $(G_0, H \cap G_0, K \cap G_0)$ is one of 28 ‘‘sporadic’’ cases recorded in [20, Table 1.2];
- III. Both H and K are solvable and (G, H, K) is recorded in [20, Proposition 4.1].

Since Theorem 1 gives a sharp lower bound on $|H|$ for each Type I factorization, it remains to consider the Type II and III factorizations. For $j = 1, \dots, 28$, a *Type II.j factorization* satisfies the conditions of Case j in [20, Table 1.2].

Lemma 3.2. *Let G be an almost simple classical group with socle G_0 and suppose $G = HK$ is a Type II.j factorization of G . Then there exists an integer ℓ and an almost simple group G_1 with socle G_0 such that*

- (i) $G_1 = H_1K_1$ is a Type II.j factorization of G_1 ; and
- (ii) $|H_1| = \ell$ divides $|H|$,

where (G_1, H_1, K_1, ℓ) is listed in Table 6.

Proof. We inspect each case in [20, Table 1.2] in turn, using MAGMA [3] to determine the minimal order of a solvable factor and to verify the existence of the factorizations presented in Table 6 (note that in Case 20 of Table 6, $G_1 = \text{PSU}_4(3).2$ is a subgroup of $\text{PGU}_4(3)$). \square

Finally, we turn to the Type III factorizations, which are described in [20, Proposition 4.1]. The latter result partitions the possible factorizations $G = HK$ into 12 cases and we will refer to *Type III.j factorizations* accordingly, for $j = 0, 1, \dots, 11$. The Type III.0 factorizations correspond to the infinite family described in [20, Proposition 4.1(a)], which we have already handled in our analysis of Type I.1 factorizations with $n = 2$ (see Remark

Case	G_1	H_1	K_1	ℓ
1	$\mathrm{PSL}_2(11)$	C_{11}	A_5	11
2	$\mathrm{PTL}_2(16)$	$D_{34}.4$	$2.S_5$	136
3	$\mathrm{PSL}_2(19)$	$19:9$	A_5	171
4	$\mathrm{PSL}_2(29)$	$29:7$	A_5	203
5	$\mathrm{PSL}_2(59)$	$59:29$	A_5	1711
6	$\mathrm{PGL}_4(3)$	$2^4:5$	$3^3:\mathrm{GL}_3(3)$	80
7	$\mathrm{PGL}_4(3)$	$(3^3:13:3).2$	$((4 \times \mathrm{PSL}_2(9)):2).2$	2106
8	$\mathrm{PTL}_4(4)$	$(2^6:63:3).2$	$((5 \times \mathrm{PSL}_2(16)):2).2$	24192
9	$\mathrm{PSL}_5(2)$	$31:5$	$2^6:(S_3 \times \mathrm{PSL}_3(2))$	155
10	$\mathrm{PSp}_4(3)$	3_+^{1+2}	$2^4:A_5$	27
11	$\mathrm{PSp}_4(3)$	3_+^{1+2}	$2^4:A_5$	27
12	$\mathrm{PSp}_4(5)$	$5_+^{1+2}.2.A_4$	$\mathrm{PSL}_2(5^2).2$	3000
13	$\mathrm{PSp}_4(7)$	$7_+^{1+2}.2.S_4$	$\mathrm{PSL}_2(7^2).2$	16464
14	$\mathrm{PSp}_4(11)$	$11_+^{1+2}.10.A_4$	$\mathrm{PSL}_2(11^2).2$	159720
15	$\mathrm{PSp}_4(23)$	$23_+^{1+2}.20.S_4$	$\mathrm{PSL}_2(23^2).2$	6424176
16	$\mathrm{Sp}_6(2)$	$3_+^{1+2}:Q_8$	S_8	216
17	$\mathrm{PGSp}_6(3)$	$(3_+^{1+4}.2^{1+4}.D_{10}).2$	$(\mathrm{PSL}_2(27):3).2$	155520
18	$\mathrm{PSU}_3(3)$	$3_+^{1+2}:8$	$\mathrm{PSL}_2(7)$	216
19	$\mathrm{PSU}_3(5)$	$5_+^{1+2}:8$	A_7	1000
20	$\mathrm{PSU}_4(3).2$	$3^4:2$	$\mathrm{PSL}_3(4).2$	162
21	$\mathrm{PSU}_4(8).3$	$(513:3).3$	$(2^{12}.\mathrm{SL}_2(64).7).3$	4617
22	$\Omega_7(3)$	$3^3:2^4.5$	$G_2(3)$	19440
23	$\Omega_7(3)$	$3^{3+3}:13$	$\mathrm{Sp}_6(2)$	9477
24	$\Omega_9(3)$	$3^{6+4}.2^{1+4}.5$	$\Omega_8^-(3).2$	9447840
25	$\Omega_8^+(2)$	$2^2:15.4$	$\mathrm{Sp}_6(2)$	240
26	$\Omega_8^+(2)$	$2^6:15$	A_9	960
27	$\mathrm{PSO}_8^+(3)$	$3^4.4.D_{10}$	$\mathrm{SO}_7(3)$	3240
28	$\mathrm{P}\Omega_8^+(3)$	$3^6:(3^3:13)$	$\Omega_8^+(2)$	255879

TABLE 6. Type II factorizations $G_1 = H_1K_1$ with $|H_1| = \ell$ in Lemma 3.2

1(a)). The factorizations of Type III.j with $j = 1, \dots, 11$ coincide with the cases recorded in row j of [20, Table 4.1].

Lemma 3.3. *Let G be an almost simple classical group with socle G_0 and suppose $G = HK$ is a Type III.j factorization of G . Then there exists an integer ℓ and an almost simple group G_1 with socle G_0 such that*

- (i) $G_1 = H_1K_1$ is a Type III.j factorization of G_1 ; and
- (ii) $|H_1| = \ell$ divides $|H|$,

where (G_1, H_1, K_1, ℓ) is listed in Table 7.

Proof. As noted above, the Type III.0 factorizations have already been handled in our treatment of Type I.1 factorizations in Theorem 1, so we may assume $j = 1, \dots, 11$. Here the possibilities for G , H and K are listed in [20, Table 4.1] and the desired result quickly follows. \square

Proposition 3.4. *The conclusion to Theorem 2 holds if G_0 is a classical group.*

Proof. We combine Lemmas 3.2 and 3.3 with Theorem 1. \square

Case	G_1	H_1	K_1	ℓ
0	$\mathrm{PGL}_2(q)$	C_{q+1}	P_1	$q+1$
1	$\mathrm{PSL}_2(7)$	C_7	S_4	7
2	$\mathrm{PSL}_2(11)$	11:5	A_4	55
3	$\mathrm{PSL}_2(23)$	23:11	S_4	253
4	$\mathrm{PSL}_3(3)$	C_{13}	$3^2:2.S_4$	13
5	$\mathrm{PSL}_3(3)$	13:3	$\mathrm{AGL}_1(9)$	39
6	$\mathrm{PSL}_3(4).S_3$	7:3. S_3	$2^4:(3 \times D_{10}).2$	126
7	$\mathrm{PSL}_3(8).3$	73:9	$2^{3+6}:7^2:3$	657
8	$\mathrm{PSU}_3(8).3^2$	57:9	$2^{3+6}:(63:3)$	513
9	$\mathrm{PSU}_4(2)$	$2^4:5$	$3_+^{1+2}:2.A_4$	80
10	$\mathrm{PSU}_4(2)$	$2^4:D_{10}$	$3_+^{1+2}:2.A_4$	160
11	$\mathrm{PSU}_4(2).2$	$2^4:5:4$	$3_+^{1+2}:S_3, 3^3:S_3$	320

TABLE 7. Type III factorizations $G_1 = H_1K_1$ with $|H_1| = \ell$ in Lemma 3.3

Remark 3.5. There are some natural variations of the parameter $\ell(G_0)$ defined above. For example, let

$$\mathcal{A}(G_0) = \{H : G = HK, H \text{ abelian, } K \text{ core-free, } \mathrm{soc}(G) = G_0\}$$

and define $\kappa(G_0) = \min\{|H| : H \in \mathcal{A}(G_0)\}$ (set $\kappa(G_0) = 0$ if $\mathcal{A}(G_0)$ is empty). Then one can check that $\mathcal{A}(G_0)$ is nonempty if and only if

$$G_0 \in \{A_n, \mathrm{PSL}_n(q), M_{11}, M_{12}, M_{23}\}$$

and we calculate that $\kappa(G_0) = \ell(G_0)$ in each of these cases. We also find that every subgroup in $\mathcal{A}(G_0)$ is cyclic, with the exception of $C_6 \times C_2 \in \mathcal{A}(M_{12})$.

4. PROOF OF THEOREM 3

In this section we prove Theorem 3 on the exact factorizations of almost simple groups with a solvable factor. We begin with an elementary observation.

Lemma 4.1. *Let G be an almost simple group with socle G_0 and suppose $G = HK$ is an exact factorization. Then $|H \cap G_0|$ divides $|G_0 : K \cap G_0|$.*

Proof. We have $G_0H/G_0 \cong H/H \cap G_0$, $G_0K/G_0 \cong K/K \cap G_0$ and $(G_0H/G_0)(G_0K/G_0) = G/G_0$. By taking orders and rearranging, using the fact that $|G| = |H||K|$, we deduce that $\alpha|H \cap G_0||K \cap G_0| = |G_0|$, where $\alpha = |(G_0H/G_0) \cap (G_0K/G_0)|$. \square

Proposition 4.2. *The conclusion to Theorem 3 holds if G_0 is non-classical.*

Proof. Here G_0 is either a sporadic or alternating group. First assume G_0 is sporadic and $G = HK$ is a factorization. The possibilities for G , H and K are given in [20, Propositions 4.1 and 4.4] and it is routine to read off the cases with $|G| = |H||K|$. Similarly, if $G_0 = A_n$ then we apply [20, Proposition 4.3]. Here the cases arising in parts (a) and (b) of this proposition are recorded in parts (i) and (ii) of Theorem 3, and we use MAGMA [3] to determine the exact factorizations corresponding to the cases that arise in parts (c)-(f) of [20, Proposition 4.3]. Note that we can also use MAGMA to read off the exact factorizations coming from the cases recorded in the table in [20, Proposition 4.3(b)], which allows us to include the condition $H \leq \mathrm{AGL}_1(p^a)$ in part (ii) of the theorem. \square

Proposition 4.3. *The conclusion to Theorem 3 holds if G_0 is a classical group.*

Proof. We will consider the Type I, II and III factorizations in turn, as defined in Section 1. First assume $G = HK$ is a factorization of Type I, so the possibilities for G , H and K are described in Table 1. It is easy to see that there are exact factorizations in Case 1 of Table 1; for example, we can take $G = \mathrm{PGL}_n(q)$, H a Singer cycle of order $\frac{q^n-1}{q-1}$ and $K = P_1$, noting that H acts transitively on the set of 1-dimensional subspaces of the natural module for G . These cases are recorded in part (iii) of Theorem 3.

Next let us consider the Type I factorizations in Cases 3 and 4 of Table 1. Here $G_0 = \mathrm{Sp}_{2m}(q)$ with q even and $m \geq 2$. In Case 3 we have $\Omega_{2m}^-(q) \trianglelefteq K \cap G_0$, so $K \cap G_0 = \Omega_{2m}^-(q)$ or $O_{2m}^-(q)$. By the proof of Proposition 2.3 we see that q^m divides $|H \cap G_0|$ and by applying Lemma 4.1 we deduce that $G = HK$ is an exact factorization only if $K \cap G_0 = \Omega_{2m}^-(q)$.

First we claim that if m is odd then $G = \mathrm{Sp}_{2m}(q)$ admits an exact factorization $G = HK$ with $H = q^m:(q^m - 1)$ and $K = \Omega_{2m}^-(q)$. To see this, we construct H as in the proof of Proposition 2.3 and we note that $H \cap K = X \cap K$, where X is an elementary abelian normal subgroup of H of order q^m with the property that every involution in X is of type b_m (in the notation of [1]). Since there are no b -type involutions in K , it follows that $X \cap K = 1$ and thus $G = HK$ as claimed.

Next we claim that there are no exact factorizations in Case 3 when $m = 2$, which also rules out an exact factorization in Case 4. To see this, we may assume $G = G_0$, $K = \Omega_4^-(q)$ and $H \leq q^3:(q^2 - 1).2 < P_2$ has order $q^2(q^2 - 1)$. Here $H = X:C$ is the only possibility, where $X = q^2$ is an irreducible module for a Singer cycle $C < \mathrm{GL}_2(q)$, and by arguing as in the proof of Proposition 2.3 we deduce that $X = \{1\} \cup z^C$ and z is a c_2 -type involution in G . Moreover, $\mathrm{fix}(z) \geq 1$ with respect to the action of z on $\Delta = G/K$ (since $z^G \cap K$ is nonempty), so H does not act regularly on Δ and we conclude that $G \neq HK$.

It is straightforward to show that none of the other cases in Table 1 yield an exact factorization. For example, consider Case 2. Here the proof of Proposition 2.2 implies that q^3 divides $|H \cap G_0|$, but we have $\mathrm{PSp}_4(q) \trianglelefteq K \cap G_0$ and thus q^3 does not divide $|G_0 : K \cap G_0|$. Therefore, the existence of an exact factorization in this case is ruled out by Lemma 4.1. Similar reasoning applies in Cases 5–9.

Finally, let us turn to the factorizations of Type II and III. For Type III factorizations, the precise possibilities for G , H and K are listed in [20, Table 4.1] and it is easy to read off the relevant cases. Similarly, the Type II factorizations are presented in [20, Table 1.2] and with the aid of MAGMA [3] and Lemma 4.1, it is straightforward to identify the cases that yield an exact factorization. \square

5. NILPOTENT REGULAR SUBGROUPS

In this final section, we prove Theorem 4, which describes the primitive permutation groups with a nilpotent regular subgroup. We will also prove Theorem 5.

Let G be a finite primitive permutation group which contains a nilpotent regular subgroup H . Let T denote the socle of G . Recall that two groups are *class-mates* if they are isomorphic to regular subgroups of the same primitive permutation group, which is not a symmetric or alternating group in its natural action.

If G is an affine group, then T is an elementary abelian p -group for a prime p . Moreover, T is regular and thus H is a class-mate of an elementary abelian p -group as in part (ii) of Theorem 4. For the remainder, let us assume G is non-affine, so T is nonabelian. Since H is nilpotent, H does not contain a nontrivial normal subgroup of T and thus the possibilities for G and H are described in [23, Theorem 1]. Three cases arise:

- (a) G is almost simple;
- (b) G is a product-type group on Δ^d of the form $G \leq G_1 \wr S_d$, where $d \geq 2$ and $G_1 \leq \mathrm{Sym}(\Delta)$ is almost simple and primitive;

(c) G is of diagonal-type (corresponding to cases (ii) and (iii) in [23, Theorem 1]).

First we handle the diagonal-type groups in case (c). For the proof of the following proposition, we need to recall the well-known Wielandt-Kegel theorem [15, 28]: any finite group which is a product of two nilpotent groups is solvable.

Proposition 5.1. *Let G be a finite primitive permutation group with a nilpotent regular subgroup H . Then G is not of diagonal-type.*

Proof. Seeking a contradiction, first assume that G is ‘simple diagonal’ as in Theorem 1(ii) of [23]. Since H is nilpotent, it follows that $T = S^2$ for some nonabelian simple group S and there are proper subgroups $A, B < S$ such that $S = AB$ and $H = A \times B$. But A and B are nilpotent, so the factorization $S = AB$ contradicts the aforementioned Wielandt-Kegel theorem.

Finally, suppose G is ‘compound diagonal’ as in [23, Theorem 1(iii)]. Then G is a blow-up of a simple diagonal primitive group which has a nilpotent regular subgroup. But we have just ruled out the existence of such a simple diagonal group, so this case can also be eliminated. \square

To handle cases (a) and (b) above, we need the following simple lemma. Recall that the semi-dihedral and generalized quaternion groups of order 2^{e+1} are defined as follows:

$$\begin{aligned} \text{SD}_{2^{e+1}} &= \langle x, y \mid x^{2^e} = y^2 = 1, x^y = x^{2^{e-1}-1} \rangle \\ \text{Q}_{2^{e+1}} &= \langle x, y \mid x^{2^e} = y^4 = 1, x^y = x^{-1}, x^{2^{e-1}} = y^2 \rangle \end{aligned}$$

Lemma 5.2. *Let A be a nilpotent subgroup of $\text{GL}_1(q^m):m \leq \Gamma\text{L}_1(q^m)$ with $m \geq 2$. Then A is transitive on the set of nonzero vectors of \mathbb{F}_q^m if and only if*

- (i) $A = \text{GL}_1(q^m) = C_{q^m-1}$; or
- (ii) $m = 2$, q is a Mersenne prime and $A = C_{\frac{1}{2}(q-1)} \times B$ with $B = \text{SD}_{4(q+1)}$ or $\text{Q}_{2(q+1)}$.

Proof. Let Ω be the set of nonzero vectors of \mathbb{F}_q^m . Clearly, if (i) holds then A is transitive on Ω . Now assume (ii) holds. If $B = \text{SD}_{4(q+1)}$ then $A = \Gamma\text{L}_1(q^2)$ is transitive. If $B = \text{Q}_{2(q+1)}$ then both A and B have a unique involution, which lies in $\text{GL}_1(q^2)$ and fixes no nonzero vector of \mathbb{F}_q^2 . It follows that A acts regularly on Ω .

For the remainder, we may assume that A acts transitively on Ω . In particular, $|A|$ is divisible by $q^m - 1$.

First assume that $q^m - 1$ has a primitive prime divisor r and let $a \in A$ be of order r . Let R be the unique Sylow r -subgroup of A and note that R is cyclic since $r > m$. Since A is nilpotent, we have $A = R \times S$, where S is a Hall r' -subgroup of A , and thus $a \in Z(A)$. Therefore,

$$A = C_A(a) \leq C_{\text{GL}_1(q^m):m}(a) = \text{GL}_1(q^m)$$

and thus (i) holds.

To complete the proof, let us now assume that $q^m - 1$ does not have a primitive prime divisor. Then either $q^m = 2^6$, or $m = 2$ and q is a Mersenne prime. In the former case, it is straightforward to check that (i) holds, so assume $m = 2$ and q is a Mersenne prime. Write $\text{GL}_1(q^2).2 = \Gamma\text{L}_1(q^2) = \langle x \rangle : \langle y \rangle = C_{q^2-1} : C_2$ with $x^y = x^q$. Since $q+1$ is a power of 2, we have $q^2 - 1 = 2(q+1) \cdot \frac{1}{2}(q-1)$ and $\frac{1}{2}(q-1)$ is odd. Let $x_1 = x^{2(q+1)}$ and $x_2 = x^{\frac{1}{2}(q-1)}$. Then $|x_1| = \frac{1}{2}(q-1)$, $|x_2| = 2(q+1)$ and $\langle x \rangle = \langle x_1 \rangle \times \langle x_2 \rangle$. Now $x_1^y = x_1^q = x_1$ and $x_2^y = x_2^q$, so

$$\Gamma\text{L}_1(q^2) = \langle x_1, x_2, y \rangle = \langle x_1 \rangle \times \langle x_2, y \rangle = C_{\frac{1}{2}(q-1)} \times \text{SD}_{4(q+1)}$$

is nilpotent. Finally, set $z = x_2y$ and note that $z^2 = x_2yx_2y = x_2^{q+1}$. Since $|x_2| = 2(q+1)$, it follows that z has order 4 and we deduce that

$$\langle x_1 \rangle \times \langle x_2^2, x_2y \rangle = C_{\frac{1}{2}(q-1)} \times Q_{2(q+1)}.$$

This completes the proof. \square

In order to determine the almost simple candidates from Theorem 3, we need the following projective version of Lemma 5.2. In the statement, we write $\frac{q^m-1}{q-1}:mf$ for the image of $\text{GL}_1(q^m):mf < \text{GL}_m(q)$ modulo scalars, where $q = p^f$ with p prime.

Lemma 5.3. *Let A be a nilpotent subgroup of $\frac{q^m-1}{q-1}:mf$ with $m \geq 2$. Then A is transitive on the set of 1-dimensional subspaces of \mathbb{F}_q^m if and only if one of the following holds:*

- (i) A is a cyclic group of order $\frac{q^m-1}{q-1}$.
- (ii) $m = 2$, q is a Mersenne prime and $A = D_{2(q+1)}$ or D_{q+1} .
- (iii) $m = 2$, $q = 8$ and $A = 3_-^{1+2}$.

In (ii), we note that $\frac{q^m-1}{q-1}:mf = D_{2(q+1)}$ has two subgroups isomorphic to D_{q+1} ; one is transitive, the other is intransitive.

Proof. This is very similar to the proof of the previous lemma. Suppose A is transitive, so $|A|$ is divisible by $\frac{q^m-1}{q-1}$. If there exists a primitive prime divisor r of $p^{mf} - 1$, then by considering the centralizer of an element in A of order r we deduce that (i) holds. Now assume $p^{mf} - 1$ does not have a primitive prime divisor, so either $p^{mf} = 2^6$, or $m = 2$ and q is a Mersenne prime. In the former case, $q \in \{2, 4, 8\}$ and it is straightforward to check that either (i) holds, or $q = 8$ and $A < C_9:C_6 < \text{P}\Gamma\text{L}_2(8)$ is an extraspecial group of type 3_-^{1+2} as in (iii). Finally, if $m = 2$ and q is a Mersenne prime, then $\frac{q^m-1}{q-1}:mf = D_{2(q+1)}$ and we deduce that (i) or (ii) holds. Specifically, if $D_{2(q+1)} = \langle x, y \rangle$, where $|x| = q+1$ and y is an involution fixing a 1-space, then $D_{q+1} = \langle x^2, xy \rangle$ is transitive and $D_{q+1} = \langle x^2, y \rangle$ is intransitive. \square

Next we establish a key result for the analysis of product-type groups.

Proposition 5.4. *Let G be an almost simple primitive group of degree n with socle G_0 and suppose H is a nilpotent transitive subgroup of G . Then one of the following holds:*

- (i) G is 2-transitive and $H = C_n$ is regular.
- (ii) $G_0 = A_n$ and H is transitive on $\{1, \dots, n\}$.
- (iii) $G_0 = \text{PSL}_2(q)$, $n = q+1$ and $H = D_{2(q+1)}$ or D_{q+1} , where q is a Mersenne prime.
- (iv) $(G, H, n) = (\text{P}\Gamma\text{L}_2(8), 3_-^{1+2}, 9)$, $(M_{12}, C_6 \times C_2, 12)$ or $(M_{24}, D_8 \times C_3, 24)$.
- (v) $G_0 = \text{PSP}_4(3)$, $n = 27$ and $H = 3_{\pm}^{1+2}$ or 3.3_+^{1+2} .

In particular, G is 2-transitive in cases (i)–(iv).

Proof. Since we have a factorization $G = HK$, where K is a point stabilizer, we can proceed by inspecting the possibilities for (G, H) determined in [20]. Set $\Delta = G/K$.

Set $H_0 = H \cap G_0$ and first assume G_0 is a classical group over \mathbb{F}_q , where $q = p^f$ with p a prime. We consider Type I, II and III factorizations in turn (see Section 1 for the definitions). To begin with, let us assume $G = HK$ is a Type I factorization, in which case the possibilities for G and H are described in Table 1. Let $A \leq G_0$ be the overgroup of H_0 given in Table 1.

First consider Case 1 of Table 1. Here $G_0 = \text{PSL}_m(q)$ and $H \leq \frac{q^m-1}{q-1}:mf$ acts transitively on Δ , which we identify with the set of 1-dimensional subspaces of \mathbb{F}_q^m . Now G acts

2-transitively on Δ and by applying Lemma 5.3, we deduce that either (i) or (iii) holds, or we are in the special case $(G, H, n) = (\text{PTL}_2(8), 3_-^{1+2}, 9)$ recorded in (iv).

Now consider Case 2 of Table 1, so $G_0 = \text{PSL}_4(q)$ and $A = q^3 : \frac{q^3-1}{d} : 3$ with $d = (4, q-1)$. By Theorem 1, we know that $|H|$ is divisible by $q^3(q^3-1)/(2, q-1)$. Now

$$H < P_1 \leq \text{AFL}_3(q) = q^3 : (\text{GL}_3(q).f)$$

and $O_p(H) = O_p(P_1)$ is the full unipotent radical of the parabolic subgroup P_1 (here $O_p(H)$ denotes the largest normal p -subgroup of H). It follows that $H \leq \text{AFL}_1(q^3) = q^3 : \text{FL}_1(q^3)$. But $\text{AGL}_1(q^3) = q^3 : C_{q^3-1}$ is a Frobenius group, and so is $H \cap \text{AGL}_1(q^3)$, whence H is not nilpotent and we have reached a contradiction.

Next let us turn to Case 3 of Table 1, so $G_0 = \text{Sp}_{2m}(q)$ and $A = q^{\frac{1}{2}m(m+1)} : (q^m - 1).m$ with q even. By Theorem 1, $|H|$ is divisible by $q^m(q^m - 1)$. Let $L = H/O_2(H)$ and note that $O_2(H)$ is elementary abelian. In addition, observe that $K \cap G_0 = O_{2m}^-(q)$ since K is a maximal subgroup of G . Then

$$L \leq \text{FL}_1(q^m) = \text{GL}_1(2^{mf}).mf$$

and since $q = 2^f$ is even, we deduce that $L = C_{q^m-1}$ is cyclic by Lemma 5.2. Since H is nilpotent, it follows that $H = O_2(H) \times C_{q^m-1}$ is abelian and therefore regular on Δ . But this is incompatible with Theorem 3 (specifically, the condition $K \cap G_0 = O_{2m}^-(q)$ in part (iv) of Theorem 3). Similar reasoning eliminates all the other cases in Table 1.

Next assume $G = HK$ is a Type II factorization. Here the possibilities for (G, H) are listed in [20, Table 1.2], which gives an overgroup $A \leq G_0$ of H_0 . In addition, by Lemma 3.2, $|H|$ is divisible by the integer ℓ in Table 6. With the exception of Case 1 (which is 2-transitive) and Cases 10 and 11 (which give rise to the examples recorded in part (v) of the proposition), it is straightforward to check that H does not contain a nilpotent subgroup of order divisible by ℓ . Similarly, if $G = HK$ is a Type III factorization, then the desired result follows immediately from [20, Proposition 4.1] (note that G is 2-transitive in the cases labelled 0, 1 and 4 in Table 7).

To complete the proof, we may assume G_0 is a sporadic or alternating group (recall that no almost simple exceptional group of Lie type admits a solvable factor). For G_0 sporadic, we apply [20, Proposition 4.4], which gives rise to the two examples appearing in part (iv). Finally, let us assume $G_0 = A_n$ is an alternating group. Here we apply [20, Proposition 4.3], which describes the possibilities for (G, H) . We will refer to cases (a)–(f) of [20, Proposition 4.3]. Clearly, (ii) holds in case (a), and H is not nilpotent in (c). Cases (d) and (e) can be checked directly; there is an example with $G = S_6$, $H = C_6$ and $K = \text{PGL}_2(5)$, but here the action of G on Δ is 2-transitive and (i) holds. Similarly, in (f) the only valid possibility is $G = A_8$, $H = C_{15}$ and $K = \text{AGL}_3(2)$, and once again we find that G is 2-transitive. Finally, let us consider part (b). Here $G = S_n$ or A_n , $K = (S_{n-2} \times S_2) \cap G$ and $n = p^a$ is a prime power. Moreover, the nilpotency of H implies that $H \leq \text{AFL}_1(p^a) = p^a : (\text{GL}_1(p^a).a)$, and $|H|$ must be divisible by $|G : K| = \frac{1}{2}p^a(p^a - 1)$. It follows that $O_p(H) = p^a$ and $H/O_p(H) \leq \text{GL}_1(p^a).a$ contains a nontrivial element of $\text{GL}_1(p^a)$, which does not centralize $O_p(H)$. This contradicts the nilpotency of H and the proof is complete. \square

By combining the previous result (and its proof) with Theorem 3, it is straightforward to read off the almost simple primitive groups with a nilpotent regular subgroup.

Corollary 5.5. *Let G be an almost simple primitive group of degree n with socle G_0 and suppose H is a nilpotent regular subgroup of G . Then one of the following holds:*

- (i) $G_0 = A_n$ and H is transitive on $\{1, \dots, n\}$.
- (ii) $G_0 = \text{PSL}_a(q)$ and H is a cyclic group of order $\frac{q^a-1}{q-1}$.

- (iii) $G_0 = \text{PSL}_2(q)$ and $H = D_{q+1}$, where q is a Mersenne prime.
- (iv) (G, H) is one of the following:
 $(\text{PSL}_2(11), C_{11})$, (M_{11}, C_{11}) , $(M_{12}, C_6 \times C_2)$, (M_{23}, C_{23}) or $(M_{24}, D_8 \times C_3)$.
- (v) $G_0 = \text{PSP}_4(3)$ and $H = 3_{\pm}^{1+2}$.

Proposition 5.6. *Let $G \leq G_1 \wr S_d$ be a primitive product-type group, where G_1 is almost simple and primitive. If G has a nilpotent regular subgroup, then either G_1 is 2-transitive, or G_1 has socle $\text{PSP}_4(3)$ acting on 27 points.*

Proof. By [23, Proposition 2.5], G_1 has a nilpotent transitive subgroup. Then Proposition 5.4 implies that either G_1 is 2-transitive, or G_1 has socle $\text{PSP}_4(3)$ and a regular subgroup 3_+^{1+2} . The result follows. \square

We have already noted that $(3_{\pm}^{1+2})^d$ is a regular subgroup of $\text{PSP}_4(3) \wr S_d$ in its product action of degree 27^d . However, $\text{PSP}_4(3) \wr S_d$ is *not* the blow-up of a 2-transitive group (since the action of $\text{PSP}_4(3)$ on the set of cosets of $2^4:A_5$ is simply primitive) and thus $(3_{\pm}^{1+2})^d$ is *not* a generalized B-group.

Example 5.7. We claim that the primitive group $\text{PSP}_4(3) \wr S_d$ in its product action of degree 27^d has a regular subgroup isomorphic to $(3_+^{1+2})^e \times (3^6:3_+^{1+2})^f$ for any non-negative integers e and f with $e + 3f = d$.

To see this, we may assume that $e = 0$ and $f = 1$, so $d = 3$. Let $P_i = X_i:Y_i \cong 3_+^{1+2}$, where $1 \leq i \leq 3$, $X_i \cong C_3^2$ and $Y_i = \langle y_i \rangle \cong C_3$. Let

$$(P_1 \times P_2 \times P_3):\langle \pi \rangle \cong 3_+^{1+2} \wr C_3,$$

where $\pi : y_1 \mapsto y_2, y_2 \mapsto y_3$ and $y_3 \mapsto y_1$, and set

$$H = (X_1 \times X_2 \times X_3):(\langle y_1 y_2^{-1}, y_2 y_3^{-1} \rangle : \langle y_1 y_2 y_3 \pi \rangle).$$

Then $\langle y_1 y_2^{-1}, y_2 y_3^{-1} \rangle : \langle y_1 y_2 y_3 \pi \rangle \cong 3_+^{1+2}$ and $H \cong 3^6:3_+^{1+2}$. Suppose that $y_1 y_2 y_3 \pi$ fixes a point $x_1 x_2 x_3$. Then

$$x_1 x_2 x_3 = (x_1 x_2 x_3)^{y_1 y_2 y_3 \pi} = (x_1 y_1 x_2 y_2 x_3 y_3)^{\pi} = x_2 y_2 x_3 y_3 x_1 y_1$$

and thus $y_1 y_2 y_3 = 1$, which is not possible. It follows that H is regular and this justifies the claim.

We remark that $\text{PSP}_4(3) \wr S_d$ appears to have many regular subgroups in its product action of degree 27^d . For example, if $d = 2$ then a MAGMA calculation shows that there are 19 conjugacy classes of regular subgroups (13 up to isomorphism).

Finally, we are ready to prove Theorems 4 and 5.

Proof of Theorem 4. Let G be a finite primitive permutation group of degree n with socle T and a nilpotent regular subgroup H . Then by the observations made at the beginning of this section, together with Propositions 5.1 and 5.6, we deduce that one of the following holds:

- (a) G is affine;
- (b) $G \leq G_1 \wr S_d$ is of product-type, where G_1 is a primitive group with socle $\text{PSP}_4(3)$ acting on 27 points;
- (c) G is a blow-up of an almost simple 2-transitive group.

If G is an affine group of degree p^d with p prime and $d \geq 1$, then H is a class-mate of C_p^d as in part (ii) of Theorem 4. Similarly, if (b) holds then H is a class-mate of $(3_+^{1+2})^d$ as in part (iv) of Theorem 4. To complete the proof, we may assume that (c) holds.

Let us first assume G is almost simple. By applying Corollary 5.5, either $T = A_n$ and H is any nilpotent group of order n as in part (i) of Theorem 4, or G is one of the groups described in part (iii) of Theorem 4 (with $d = 1$).

Finally, suppose $G \leq G_1 \wr S_d$ is a blow-up of an almost simple 2-transitive group G_1 of degree m , so $n = m^d$ with $d \geq 2$. Write $T = S^d$, where S is the socle of G_1 . As observed in the proof of Proposition 5.6, G_1 has a nilpotent transitive subgroup H_1 and therefore the possibilities for G_1 and H_1 are described in Proposition 5.4. We inspect each case in turn.

First assume that $H_1 = C_m$ as in part (i) of Proposition 5.4. Then H_1 is regular and thus G_1 is one of the groups in parts (i), (ii) or (iv) of Corollary 5.5. We deduce that H is a class-mate of C_m^d and either $S = A_m$, or $(S, m) = (\text{PSL}_a(q), \frac{q^a-1}{q-1})$, $(\text{PSL}_2(11), 11)$, $(M_{11}, 11)$ or $(M_{23}, 23)$. All of these cases appear in part (iii)(a) of Theorem 4.

Next suppose G_1 and H_1 are as in part (ii) of Proposition 5.4. Here $S = A_m$ and H is a class-mate of C_m^d , which we have already noted is one of the cases in part (iii)(a) of Theorem 4. Similarly, if part (iii) of Proposition 5.4 is satisfied, then $S = \text{PSL}_2(q)$, $m = q + 1$ and H is a class-mate of C_m^d . Finally, if G_1 and H_1 are as in part (iv) of Proposition 5.4 then either $S = \text{PSL}_2(8)$ and H is a class-mate of C_9^d , or $S = M_{12}$ or M_{24} and H is a class-mate of $(C_6 \times C_2)^d$ or $(D_8 \times C_3)^d$, respectively. All of these cases are covered by part (iii) of Theorem 4. This completes the proof. \square

Proof of Theorem 5. Let H be a finite nilpotent group and let G be a primitive permutation group containing H as a regular subgroup. Then as explained in the first paragraph in the proof of Theorem 4, G is either affine (and thus H is a class-mate of C_p^d for some prime p and $d \geq 1$), or G is a blow-up of an almost simple primitive group with socle $\text{PSp}_4(3)$ acting on 27 points (in which case H is a class-mate of $(3_+^{1+2})^d$), or G is the blow-up of a 2-transitive group. The desired conclusion follows immediately. \square

REFERENCES

- [1] M. Aschbacher and G.M. Seitz, *Involutions in Chevalley groups over fields of even order*, Nagoya Math. J. **63** (1976), 1–91.
- [2] B. Baumeister, *Primitive permutation groups with a regular subgroup*, J. Algebra **310** (2007), 569–618.
- [3] W. Bosma, J. Cannon and C. Playoust, *The MAGMA algebra system I: The user language*, J. Symb. Comput. **24** (1997), 235–265.
- [4] J.N. Bray, D.F. Holt and C.M. Roney-Dougal, *The Maximal Subgroups of the Low-dimensional Finite Classical Groups*, London Math. Soc. Lecture Note Series, vol. 407, Cambridge University Press, 2013.
- [5] T.C. Burness and M. Giudici, *Classical groups, derangements and primes*, Aust. Math. Soc. Lecture Series, vol. 25, Cambridge University Press, 2016.
- [6] W. Burnside, *Theory of groups of finite order*, Dover Publications Inc., New York, 1955, reprint of 2nd edition, Cambridge University Press, 1911.
- [7] M. Giudici, *Factorisations of sporadic simple groups*, J. Algebra **304** (2006), 311–323.
- [8] R.M. Guralnick and J. Saxl, *Monodromy groups of polynomials*, in Groups of Lie type and their geometries (Como, 1993), 125–150, London Math. Soc. Lecture Note Ser., 207, Cambridge Univ. Press, Cambridge, 1995.
- [9] P. Hegedus, *Regular subgroups of the affine group*, J. Algebra **225** (2000), 740–742.
- [10] C. Hering, M.W. Liebeck and J. Saxl, *The factorizations of the finite exceptional groups of Lie type*, J. Algebra **106** (1987), 517–527.
- [11] N. Itô, *On the factorizations of the linear fractional groups $LF(2, p^n)$* , Acta. Sci. Math. Szeged **15** (1953), 79–84.
- [12] G. Jones, *Cyclic regular subgroups of primitive permutation groups*, J. Group Theory **5** (2002), 403–407.
- [13] W.M. Kantor, *k -homogeneous groups*, Math. Z. **124** (1972), 261–265.
- [14] L.S. Kazarin, *Groups that can be represented as a product of two solvable subgroups*, Comm. Algebra **14** (1986), 1001–1066.
- [15] O.H. Kegel, *Produkte nilpotenter Gruppen*, Arch. Math. **12** (1961), 90–93.

- [16] P.B. Kleidman and M.W. Liebeck, *The Subgroup Structure of the Finite Classical Groups*, London Math. Soc. Lecture Note Series, vol. 129, Cambridge University Press, 1990.
- [17] C.H. Li, *The finite primitive permutation groups containing an abelian regular subgroup*, Proc. London Math. Soc. **87** (2003), 725–747.
- [18] C.H. Li, Z.P. Lu and J.M. Pan, *Finite vertex-primitive edge-transitive metacirculants*, J. Algebraic Combin. **40** (2014), 785–804.
- [19] C.H. Li and B. Xia, *Factorizations of almost simple groups with a factor having many non-solvable composition factors*, J. Algebra **528** (2019), 439–473.
- [20] C.H. Li and B. Xia, *Factorizations of almost simple groups with a solvable factor, and Cayley graphs of solvable groups*, Mem. Amer. Math. Soc., to appear.
- [21] M.W. Liebeck, C.E. Praeger and J. Saxl, *The maximal factorizations of the finite simple groups and their automorphism groups*, Mem. Amer. Math. Soc. **432** (1990), iv+151 pp.
- [22] M.W. Liebeck, C.E. Praeger and J. Saxl, *On factorizations of almost simple groups*, J. Algebra **185** (1996), 409–419.
- [23] M.W. Liebeck, C.E. Praeger and J. Saxl, *Transitive subgroups of primitive permutation groups*, J. Algebra **234** (2000), 291–361.
- [24] M.W. Liebeck, C.E. Praeger and J. Saxl, *Regular subgroups of primitive permutation groups*, Mem. Amer. Math. Soc. **203** (2010), no. 952, vi+74 pp.
- [25] I. Schur, *Zur Theorie der einfach transitiven Permutationsgruppen*, S. B. Preuss. Akad. Wiss., Phys.-Math. Kl. (1933), 598–623.
- [26] J. Wiegold and A.G. Williamson, *The factorisation of the alternating and symmetric groups*, Math. Z. **175** (1980), 171–179.
- [27] H. Wielandt, *Finite permutation groups*, Academic Press, New York-London, 1964.
- [28] H. Wielandt, *Über Produkte von nilpotenten Gruppen*, Illinois J. Math. **2** (1958), 611–618.
- [29] M. Wildon, *Permutation groups containing a regular abelian subgroup: the tangled history of two mistakes of Burnside*, Math. Proc. Camb. Phil. Soc. **168** (2020), 613–633.
- [30] K. Zsigmondy, *Zur Theorie der Potenzreste*, Monatsh. Math. Phys. **3** (1892), 265–284.

T.C. BURNES, SCHOOL OF MATHEMATICS, UNIVERSITY OF BRISTOL, BRISTOL BS8 1UG, UK

Email address: t.burness@bristol.ac.uk

C.H. LI, SUSTECH INTERNATIONAL CENTER FOR MATHEMATICS, SOUTHERN UNIVERSITY OF SCIENCE AND TECHNOLOGY, SHENZHEN 518055, GUANGDONG, P.R. CHINA

Email address: lich@sustech.edu.cn