Journal of Algebra 367 (2012) 222–236

Contents lists available at SciVerse ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra

On prime power order elements of general linear groups

Joseph DiMuro

Biola University, 13800 Biola Ave., La Mirada, CA 90639, United States

ARTICLE INFO

Article history:
Received 1 April 2011
Available online 27 June 2012
Communicated by Martin Liebeck

MSC:
20D05
20D06
20D08

Keywords:
Representation theory
Lie groups

ABSTRACT

We will classify the absolutely irreducible subgroups $G \leqslant GL_d(q)$ which are not realizable modulo scalars over any proper subfield of $GF(q)$, which are "nearly simple", and which contain elements of prime power order greater than $d/3$.

1. Introduction

Let G be a subgroup of the general linear group $GL_d(q)$, where $d \geqslant 2$ and $q = p^a$ (p prime). Let g be an element of G of prime power order r; $r = t^c$, where $t \neq p$ is prime. Extending the notation in [5], we will call g a pppd$(d, q; e)$ element of $GL_d(q)$ if r is a primitive divisor of $q^e - 1$, where $e \geqslant 1$. That is, r divides $q^e - 1$, but r does not divide $q^{e'} - 1$ for any e' such that $1 \leqslant e' < e$. (Here, "pppd" stands for "primitive prime power divisor".)

In [2], I classified all subgroups $G \leqslant GL_d(q)$ which contain a pppd$(d, q; e)$ element for some $e \geqslant \lfloor d/3 \rfloor$, where $e \geqslant 2$. (This extended the results in [5], where the element g was required to have prime order, and it was also required that $e > d/2$.) If we treat $GL_d(q)$ as acting on a vector space V (over $GF(q)$) of dimension d, then such a pppd$(d, q; e)$ element will act irreducibly on a subspace of dimension e.

Further, if a pppd$(d, q; e)$ element g (where $e \geqslant \lfloor d/3 \rfloor$) has order r, then we must have $r > d/3$; if r is a primitive divisor of $q^e - 1$, then e must divide $\phi(r) \leqslant r - 1$ (where ϕ is Euler's totient). Thus, $r \geqslant e + 1 > d/3$. In [2], all subgroups $G \leqslant GL_d(q)$ containing a prime power order element of order $r > d/3$ were classified; then those subgroups for which $e \geqslant \lfloor d/3 \rfloor$ were identified.

E-mail address: joseph.dimuro@biola.edu.

0021-8693/$ – see front matter
http://dx.doi.org/10.1016/j.jalgebra.2012.03.044

Table 1
$S = A_n$.

G'	d	p	r	G'	d	p	r
A_5	2	2	3, 4, 5	$3 \cdot A_7$	3	5	3, 4, 5, 7
	3	$p \neq 2, 5$	3, 4, 5		6	$p \neq 3$	3, 4, 5, 7
	5	$p \geqslant 5$	3, 4, 5		9	7	4, 5, 7
$2 \cdot A_5$	2	$p \neq 2$	3, 4, 5		15	$p \neq 3$	7
	4	$p \geqslant 5$	3, 4, 5		18	5	7
	6	$p \neq 2, 5$	3, 4, 5	$6 \cdot A_7$	6	$p \geqslant 5$	3, 4, 5, 7
A_6	3	3	3, 4, 5, 8		12	5	5, 7
	8	$p \neq 3$	3, 4, 5, 8	A_8	4	2	3, 4, 5, 7, 8
	9	$p \neq 2, 5$	4, 5, 8		13	3, 5	5, 7, 8
	10	$p \geqslant 5$	4, 5, 8		14	$p \neq 3, 5$	5, 7, 8
$2 \cdot A_6$	2	3	3, 4, 5, 8		19	7	7, 8
	4	$p \geqslant 5$	3, 4, 5, 8		20	$p \neq 3, 7$	7, 8
	6	3	3, 4, 5, 8		21	$p \neq 2$	8
	8	$p \geqslant 7$	3, 4, 5, 8	$2 \cdot A_8$	8	$p \neq 2$	3, 4, 5, 7, 8
	10	$p \geqslant 5$	4, 5, 8		16	7	7, 8
$3 \cdot A_6$	3	$p \neq 3$	3, 4, 5, 8	A_9	8	2	3, 4, 5, 7, 8, 9
	6	$p \geqslant 5$	3, 4, 5, 8		19	7	7, 8, 9
	9	$p \neq 3, 5$	4, 5, 8		20	2	7, 8, 9
	15	$p \geqslant 5$	8		21	$p \neq 2$	8, 9
$6 \cdot A_6$	6	$p \geqslant 5$	3, 4, 5, 8		26	2	9
	12	$p \geqslant 7$	5, 8	$2 \cdot A_9$	8	$p \neq 2$	3, 4, 5, 7, 8, 9
A_7	4	2	3, 4, 5, 7	A_{10}	16	2	7, 8, 9
	8	5	3, 4, 5, 7		26	2	9
	10	$p \neq 2$	4, 5, 7	$2 \cdot A_{10}$	8	5	3, 4, 5, 7, 8, 9
	13	3, 5	5, 7		16	$p \neq 2, 5$	7, 8, 9
	14	$p \neq 3, 5$	5, 7	A_{11}	16	2	7, 8, 9, 11
	15	$p \neq 2, 7$	7	$2 \cdot A_{11}$	16	$p \neq 2$	7, 8, 9, 11
	20	2	7	A_{12}	16	2	7, 8, 9, 11
$2 \cdot A_7$	4	$p \neq 2$	3, 4, 5, 7	$2 \cdot A_{12}$	16	3	7, 8, 9, 11
	6	3	3, 4, 5, 7		32	$p \geqslant 5$	11
	14	$p \geqslant 5$	5, 7	A_{13}	32	2	11, 13
	16	7	7	$2 \cdot A_{13}$	32	$p \neq 2$	11, 13
	20	$p \geqslant 5$	7	$2 \cdot A_{14}$	32	7	11, 13

Given an integer $d \geqslant 2$ and a prime power $q = p^a$, let Z be the subgroup of $GL_d(q)$ consisting of all scalar matrices. Given $G \leqslant GL_d(q)$, we will say that G is realizable modulo scalars over $GF(q_0)$ (where $q_0 \leqslant q$ is a power of p) if $G \leqslant GL_d(q_0) \circ Z$. We will prove the following:

Theorem 1.1. *Let $G \leqslant GL_d(q)$ be an absolutely irreducible subgroup that is not realizable modulo scalars over any proper sub field of $GF(q)$. Assume that $S \leqslant G/(G \cap Z) \leqslant \mathrm{Aut}(S)$ for some nonabelian simple group S. Let $r = t^c$ be a prime power (t prime) for which there exists an element $g_r \in G/(G \cap Z)$ of order r.*

If $d \geqslant 2$, $r > d/3$, and $r \neq 2$, then one of the following occurs:

- *S is a Lie type group in characteristic p.*
- *S is any other nonabelian finite simple group*; *then either V is the deleted permutation module for A_n and S_n (these modules arise for any $n \geqslant 5$), or G' is listed in Tables 1 through 5.*

Note: there do not seem to be any meaningful results in the case where S is a Lie type group in characteristic p, unless the value of e is also taken into account. One example from [5] (where it is required that r is prime and $e > d/2$) will suffice to explain why:

Assume that $S = L_l(p^b)$, for some positive integer b. Assume that G is not realizable modulo scalars over any proper subfield of $GF(q)$. It is shown in [11] that we must then have $b = af$ (for some integer f), and $\dim V = (\dim M)^f$, where M is an S-module of dimension at least l over the algebraic closure of $GF(p)$. It is shown in [5] that r divides $q^{xf} - 1$ for some $1 \leqslant x \leqslant l$. So for fixed values of d, l, and f, examples where r is large compared to d can be found easily enough, simply by taking q sufficiently

Table 2
S is a sporadic group.

G'	d	r	p	G'	d	r	p
M_{11}	5	3, 4, 5, 8, 11	3	J_1	20	7, 11, 19	2
	9	4, 5, 8, 11	11		31, 45	11, 19	7
	10	4, 5, 8, 11	–		7, 14, 27, 49	3, 5, 7, 11, 19	11
	11	4, 5, 8, 11	$p \neq 2, 3$		22, 34, 43, 55	11, 19	19
	16	8, 11	$p \neq 3$		56	19	$p \neq 19$
	24	11	3	J_2	6	3, 4, 5, 7, 8	2
M_{12}	10	4, 5, 8, 11	2, 3		13	5, 7, 8	3
	11	4, 5, 8, 11	$p \neq 2, 3$		14	5, 7, 8	$p \neq 3$
	15	8, 11	3		21	8	$p \neq 2$
	16	8, 11	$p \neq 3$	$2 \cdot J_2$	6	3, 4, 5, 7, 8	$p \neq 2$
	29	11	11		14	5, 7, 8	$p \neq 2$
$2 \cdot M_{12}$	6	3, 4, 5, 8, 11	3	J_3	18	8, 9, 17, 19	3
	10	4, 5, 8, 11	$p \neq 2$	$3 \cdot J_3$	9	4, 5, 8, 9, 17, 19	2
	12	5, 8, 11	$p \neq 2, 3$		18	8, 9, 17, 19	$p \neq 3$
	32	11	$p \neq 2, 3$	J_4	112	43	2
M_{22}	10	4, 5, 7, 8, 11	2	Co_1	24	9, 11, 13, 16, 23	2
	20	7, 8, 11	11	$2 \cdot Co_1$	24	9, 11, 13, 16, 23	$p \neq 2$
	21	8, 11	$p \neq 2, 11$	Co_2	22	8, 9, 11, 16, 23	2
$2 \cdot M_{22}$	10	4, 5, 7, 8, 11	$p \neq 2$		23	8, 9, 11, 16, 23	$p \neq 2$
	28	11	5	Co_3	22	8, 9, 11, 23	2, 3
$3 \cdot M_{22}$	6	3, 4, 5, 7, 8, 11	2		23	8, 9, 11, 23	$p \neq 2, 3$
	15	7, 8, 11	2	HS	20	7, 8, 11	2
	21	8, 11	$p \neq 2, 3$		21	8, 11	5
$4 \cdot M_{22}$	16	7, 8, 11	7		22	8, 11	$p \neq 2, 5$
$12 \cdot M_{22}$	24	11	11	$2 \cdot HS$	28	11	5
M_{23}	11	4, 5, 7, 8, 11, 23	2	McL	21	8, 9, 11	3, 5
	21	8, 11, 23	23		22	8, 9, 11	$p \neq 3, 5$
	22	8, 11, 23	$p \neq 2, 23$	He	50	17	7
	44	23	2	Ru	28	13, 16, 29	2
	45	23	$p \neq 2$	$2 \cdot Ru$	28	13, 16, 29	$p \neq 2$
M_{24}	11	4, 5, 7, 8, 11, 23	2	$2 \cdot Suz$	12	5, 7, 8, 9, 11, 13, 16	3
	22	8, 11, 23	3	$3 \cdot Suz$	12	5, 7, 8, 9, 11, 13, 16	2
	23	8, 11, 23	$p \neq 2, 3$	$6 \cdot Suz$	12	5, 7, 8, 9, 11, 13, 16	$p \neq 2, 3$
	44	23	2	$3 \cdot O'N$	45	16, 19, 31	7
	45	23	$p \neq 2$	$3 \cdot Fi_{22}$	27	11, 13, 16	2
				Ly	111	67	5

large. (Similar situations arise when S is some other Lie type group in characteristic p.) So it appears that consideration of the value of e is essential to obtain meaningful results.

2. Preliminary lemmas

In proving the main theorem, a few preliminary lemmas will be needed. Most of these are number theoretic lemmas.

For any natural number n, we will denote by $\phi_n(x)$ the nth cyclotomic polynomial (the minimal polynomial of the primitive nth roots of unity). For s a natural number and p a prime, we will let $o_p(s)$ represent the multiplicative order of s modulo p. (By convention, if p divides s, we will say that $o_p(s) = 0$.) We will let s_p represent the p-part of s, and if $s_p = p^\alpha$, then we will write $p^\alpha \| s$. Finally, $v_p(s)$ will represent the natural number where $p^{v_p(s)} = s_p$. (Thus, for any s, we have $p^{v_p(s)} \| s$.)

Lemma 2.1. *Let p be a prime, and let s, n be natural numbers ($s \geqslant 2$) where $p|(s-1)$. Then with one exception, $p^\alpha \| (s^n - 1)$ iff $p^\alpha \| (n(s-1))$. The exception: if $p = 2$, n is even, and $s \equiv 3 \pmod 4$, then $p^\alpha \| (s^n - 1)$ iff $p^\alpha \| (n(s+1))$.*

Note: even in the exceptional case, if $p|(s-1)$ and $p^\alpha \| (n(s-1))$, we do have $p^\alpha | (s^n - 1)$. (In the exceptional case, it is possible that $p^\beta \| (s^n - 1)$ for some $\beta > \alpha$.)

Table 3
S is a cross-characteristic untwisted Lie group.

G'	d	p	r	G'	d	p	r
$PSp_8(2)$	35	–	17	$L_5(2)$	29	31	16
	50	3	17		30	$p \neq 2, 31$	16
$PSp_8(3)$	40	2	16	$L_3(3)$	11	13	4, 8
	41	$p \geqslant 5$	16		12	$p \neq 3, 13$	8
$2 \cdot PSp_8(3)$	40	$p \geqslant 5$	16		13	$p \neq 2, 3$	8
$PSp_6(2)$	7	–	3, 4, 5, 7, 8, 9		16	–	8, 13
	14	3	5, 7, 8, 9		26	–	13
	15	$p \neq 2, 3$	7, 8, 9		27	$p \neq 2, 3, 13$	13
	21	–	8, 9	$L_4(3)$	26	–	9, 13
	26	7	9	$L_3(4)$	15	3	7, 8
$2 \cdot PSp_6(2)$	8	–	3, 4, 5, 7, 8, 9		19	3, 7	7, 8
$PSp_6(3)$	13	–	8, 9		20	$p \neq 2, 3, 7$	7, 8
$2 \cdot PSp_6(3)$	14	$p \geqslant 5$	8, 9	$2 \cdot L_3(4)$	6	3	3,4,5,7,8
$PSp_6(5)$	62	–	25		10	–	4, 5, 7, 8
$2 \cdot PSp_6(5)$	63	$p \neq 2, 5$	25		22	3	8
$PSp_4(4)$	18	–	8, 16, 17	$3 \cdot L_3(4)$	15	$p \neq 2, 3$	7,8
	33	5	16, 17		21	$p \geqslant 5$	8
	34	$p \neq 2, 5$	16, 17	$4 \cdot L_3(4)$	4	3	3, 4, 5, 7, 8
	49	17	17		8	–	3, 4, 5, 7, 8
	50	$p \neq 2, 17$	17		16	3	7, 8
$PSp_4(5)$	12	2	8		20	$p \neq 2, 3$	7, 8
	13	$p \neq 2, 5$	8	$6 \cdot L_3(4)$	6	$p \neq 2, 3$	3, 4, 5, 7, 8
$2 \cdot PSp_4(5)$	12	$p \neq 2, 5$	8	$12 \cdot L_3(4)$	12	7	5,7,8
$PSp_4(7)$	24	2	16	$L_2(16)$	15	–	8
	25	$p \neq 2, 7$	16		16	$p \neq 17$	8
$2 \cdot PSp_4(7)$	24	$p \neq 2, 7$	16		17	–	8
$PSp_4(9)$	40	2	16	$L_2(27)$	26	–	9
	41	$p \geqslant 5$	16	$L_2(25)$	12	2	5, 8
$2 \cdot PSp_4(9)$	40	$p \geqslant 5$	16		13	$p \neq 2, 5$	5, 8
$2 \cdot P\Omega_8^+(2)$	8	–	3, 4, 5, 7	$2 \cdot L_2(25)$	12	$p \neq 2, 5$	5, 8
$3 \cdot \Omega_7(3)$	27	–	13	$L_2(49)$	24	2	16
$2 \cdot F_4(2)$	52	–	32		25	$p \neq 2, 7$	16
$G_2(3)$	14	–	7, 8, 9, 13	$2 \cdot L_2(49)$	24	$p \neq 2, 7$	16
$3 \cdot G_2(3)$	27	–	13	$L_2(81)$	40	2	16
$2 \cdot G_2(4)$	12	–	5, 7, 8, 13, 16		41	$p \geqslant 5$	16
				$2 \cdot L_2(81)$	40	$p \geqslant 5$	16

Proof. The result is trivial if $n = 1$, so assume $n \geqslant 2$. We have $s^n - 1 = (s-1)(s^{n-1} + s^{n-2} + \cdots + s + 1) = (s-1)[(s-1)(s^{n-2} + 2s^{n-3} + \cdots + (n-2)s + (n-1)) + n] = (s-1)[(s-1)M + n]$, say. Since p divides $s-1$, if p does not divide n, then p will not divide $(s^{n-1} + \cdots + s + 1)$. So the p-part of $s^n - 1$ will equal the p-part of $s-1$, which equals the p-part of $n(s-1)$.

So we may assume that p does divide n. Now, assume that p is odd. We will prove the result by induction on k, where $p^k \| n$.

First, say $p^1 \| n$. Since $s \equiv 1 \pmod{p}$, we have $M = s^{n-2} + 2s^{n-3} + \cdots + (n-2)s + (n-1) \equiv 1 + 2 + \cdots + (n-1) = n(n-1)/2 \equiv 0 \pmod{p}$. So p divides M. Therefore, p^2 divides $(s-1)M$, but the p-part of n is exactly p. Thus $p^1 \| (s^{n-1} + \cdots + s + 1)$. Therefore, the p-part of $s^n - 1$ equals the p-part of $p(s-1)$, which is the p-part of $n(s-1)$.

Now, assume the result is true when $p^k \| n$. Then if $p^{k+1} \| n$, then the p-part of $s^n - 1 = (s^p)^{n/p} - 1$ equals the p-part of $(n/p)(s^p - 1)$ by induction, which equals the p-part of $(n/p)(p)(s-1) = n(s-1)$. So the result holds whenever p divides n and p is odd.

Finally, now assume that $p = 2$ (so s is odd and n is even). Again, we use induction on k, where $2^k \| n$. First, assume that $2^1 \| n$. We have $s^n - 1 = (s^{n/2} - 1)(s^{n/2} + 1)$, which has the same 2-part as $(s-1)(s^{n/2} + 1)$. We have $s^{n/2} + 1 = (s+1)(s^{(n/2)-1} - s^{(n/2)-2} + \cdots - s + 1)$; the latter factor contains an odd number of odd terms, hence is odd. So $(s-1)(s^{n/2} + 1)$ has the same 2-part as $(s-1)(s+1)$. If $s \equiv 1 \pmod{4}$, then the 2-part of $(s-1)(s+1)$ equals the 2-part of $(s-1)(2)$, which equals the

Table 4
S is a cross-characteristic twisted Lie group.

G'	d	p	r	G'	d	p	r
$P\Omega_8^-(2)$	33	7	17	$U_4(2) \cong PSp_4(3)$	5, 6, 10, 15, 20	–	3, 4, 5, 8, 9
	34	$p \neq 2, 7$	17		23	5	8, 9
	50	3	17		24	$p \geqslant 7$	9
${}^2B_2(8)$	14	–	5, 7, 13	$2 \cdot U_4(2) \cong Sp_4(3)$	4	–	3, 4, 5, 8, 9
	35	–	13		20	–	8, 9
$2 \cdot {}^2B_2(8)$	8	5	4, 5, 7, 13	$U_4(3)$	20	2	7, 8, 9
	16, 24	13	7, 13		21	$p \geqslant 5$	8, 9
${}^3D_4(2)$	25	3	9, 13	$2 \cdot U_4(3)$	20	$p \geqslant 5$	7, 8, 9
	26	$p \geqslant 5$	9, 13	$3 \cdot U_4(3)$	6	2	3, 4, 5, 7, 8, 9
${}^3D_4(3)$	218	2, 73	73		15	–	7, 8, 9
${}^2F_4(2)'$	26	–	13, 16		21	$p \geqslant 5$	8, 9
	27	–	13, 16	$4 \cdot U_4(3)$	20	$p \geqslant 5$	7, 8, 9
$U_7(2)$	42	–	16	$6 \cdot U_4(3)$	6	$p \geqslant 5$	3,4,5,7,8,9
	43	$p \geqslant 5$	16	$U_3(3)$	6	–	4, 7, 8
$U_6(2)$	21	3	8, 9, 16		7	$p \geqslant 5$	4, 7, 8
	22	$p \geqslant 5$	8, 9, 16		14	–	7, 8
$3 \cdot U_6(2)$	21	$p \geqslant 5$	8, 9, 16		21	$p \geqslant 5$	8
$U_6(3)$	182	–	64	$U_3(4)$	12	–	5, 8, 16
	183	$p \geqslant 5$	64		13	$p \neq 2, 5$	5, 8, 16
$2 \cdot U_6(3)$	182	$p \geqslant 5$	64	$U_3(5)$	20	–	8
$U_5(2)$	10	–	4, 5, 8, 9, 16		21	$p \neq 2, 5$	8
	11	$p \geqslant 5$	4, 5, 8, 9, 16	$U_3(7)$	42	–	16
	43	5	16		43	$p \neq 2, 7$	16
	44	$p \neq 2, 5$	16				
$U_5(3)$	60	–	32				
	61	$p \geqslant 5$	32				

2-part of $n(s-1)$. If $s \equiv 3 \pmod 4$, then the 2-part of $(s-1)(s+1)$ equals the 2-part of $2(s+1)$, which equals the 2-part of $n(s+1)$.

Now assume the result is true when $2^k \| n$. If $2^{k+1} \| n$, then the 2-part of $s^n - 1 = (s^2)^{n/2} - 1$ equals the 2-part of $(n/2)(s^2-1)$ (since $s^2 \equiv 1 \pmod 4$). And that equals the 2-part of $n(s-1)$ (if $s \equiv 1 \pmod 4$) or $n(s+1)$ (if $s \equiv 3 \pmod 4$). So the result always holds for $p = 2$. □

This gives an alternative proof of Lemma 2.4 from [15]:

Lemma 2.2. *For any natural numbers $s \geqslant 2$ and n, and any odd prime p not dividing s, we have*:

$$v_p\left(s^n - 1\right) = \begin{cases} v_p\left(s^{o_p(s)} - 1\right) + v_p(n), & o_p(s) | n \\ 0, & \text{otherwise}. \end{cases}$$

Note: this lemma, as stated in [15] was restricted to the case where s is prime. This restriction was not necessary; the fact that s is prime was never used in the proof.

Further, this leads to an alternative proof of the following result from [15], which in turn was taken from [14]:

Lemma 2.3. *If p is a prime not dividing n, then the congruence $\phi_n(x) \equiv 0 \pmod p$ has solutions iff $p \equiv 1 \pmod n$. The solutions are exactly the numbers s with order n modulo p, and the p-parts of $s^n - 1$ and $\phi_n(s)$ are equal.*

If p does divide n, then let $n = p^\beta m$, where p does not divide m. Then $\phi_n(x) \equiv 0 \pmod p$ has solutions iff $p \equiv 1 \pmod m$. The solutions are exactly the numbers s with order m modulo p; for any such solution, if $n > 2$, $\phi_n(s)$ is divisible by p but not by p^2.

Proof. First assume that p does not divide n. If p divides $\phi_n(s)$, then p divides $s^n - 1$, so the order of s modulo p is a factor of n. If the order is actually n, then p does not divide $s^k - 1$ for any $k < n$,

Table 5
S is a cross-characteristic Lie type group-infinite families.

S	d	r	Constraints
$PSp_{2n}(5)$	$(5^n-1)/2$	$(5^n+1)/6$	n an odd prime
	$(5^n\pm1)/2$	$(5^n-1)/4$	n an odd prime
$PSp_{2n}(3)$	$(3^n\pm1)/2$	$(3^{n-1}+1)/2$	$n=2^c+1$, $c\geqslant 1$
	$(3^n\pm1)/2$	$(3^n+1)/4$	n an odd prime
	$(3^n\pm1)/2$	$(3^n-1)/2$	n an odd prime
$PSp_{2n}(s)$	$(s^n\pm1)/2$	$(s^n+1)/2$	$n=2^c\geqslant 2$, s odd; $s=u^{2^{c'}}$, u prime, $c'\geqslant 0$
$U_3(s)$	s^2-s	$(s^2-s+1)/3$	$s\equiv 2 \pmod 3$, $s\geqslant 5$
$U_n(s)$, $n\geqslant 3$, n odd	$(s^n-s)/(s+1)$	$(s^n+1)/(s+1)$	n prime
	$(s^n+1)/(s+1)$		
$U_n(3)$, $n\geqslant 6$, n even	$(3^n-1)/4$	$(3^{n-1}+1)/4$	$n-1$ prime
$U_n(2)$, $n\geqslant 6$, n even	$(2^n-1)/3$, $(2^n+2)/3$	$(2^{n-1}+1)/3$	$n-1$ prime
$L_n(2)$, $n\geqslant 6$	2^n-3, 2^n-2	$2^{n-1}-1$	$n-1$ prime
$L_n(3)$, $n\geqslant 4$	$(3^n-5)/2$	$(3^{n-1}-1)/2$	$n-1$ prime
$L_n(s)$, $n\geqslant 3$	$((s^n-1)/(s-1))-2$	$(s^n-1)/(s-1)$	n prime
	$((s^n-1)/(s-1))-1$	$(s^n-1)/(s-1)$	n prime
	$(s^n-1)/(s-1)$	$(s^n-1)/(s-1)$	n prime
$L_3(s)$	s^2+s-1, s^2+s	$(s^2+s+1)/3$	$s\equiv 1 \pmod 3$
$L_2(s)$, $s\geqslant 7$, $s\neq 9$	$(s-1)/2$	$(s+1)/6$	either s prime or $s=5^b$, b an odd prime
	$(s\pm1)/2$	$(s\pm1)/5$	$r=2^c$
	$(s\pm1)/2$	$(s-1)/4$	either s prime or $s=5^b$, b an odd prime
	$(s\pm1)/2$	$(s+1)/4$	either s prime or $s=3^b$, b an odd prime
	$(s\pm1)/2$	$(s-1)/3$	$r=2^c$
	$(s\pm1)/2$, $s-1$, s	$(s+1)/3$	either $s=2^b$, b an odd prime or $r=2^c$, s prime
	$(s\pm1)/2$, $s\pm1$, s	$(s-1)/2$	either s prime or $s=3^b$, b an odd prime
	$(s\pm1)/2$, $s\pm1$, s	$(s+1)/2$	either s prime or $s=t^{2^c}$, t prime, $c\geqslant 1$
	$(s\pm1)/2$, $s\pm1$, s	$s-1$	either $s=2^b$, b prime or s is a Fermat prime
	$(s\pm1)/2$, $s\pm1$, s	s	s prime
	$(s\pm1)/2$, $s\pm1$, s	$s+1$	either $s=2^{2^c}$, $c\geqslant 2$ or $s=8$, or s is a Mersenne prime

hence p does not divide $\phi_k(s)$ for any $k<n$. But $\phi_n(s)=(s^n-1)/(\prod_{k|n,k<n}\phi_k(s))$, so the p-part of $\phi_n(s)$ will equal the p-part of s^n-1.

But if the order of s modulo p is $k<n$, then p divides s^k-1. So if $p^\alpha\|s^n-1=(s^k)^{n/k}-1$, then $p^\alpha\|(n/k)(s^k-1)$ by Lemma 2.1. Thus $p^\alpha\|s^k-1$, since p does not divide n. But $\phi_n(s)$ is a factor of $(s^n-1)/(s^k-1)$, which is then not a multiple of p. So no s with multiplicative order (modulo p) less than n can be a solution of $\phi_n(x)\equiv 0 \pmod p$; the solutions are exactly those numbers s with order n modulo p. And if such a number s exists, then since p divides $s^{p-1}-1$, n must be a factor of $p-1$, so $p\equiv 1 \pmod n$.

Now assume that p divides n, and $n=p^\beta m$, where p does not divide m. Say $\beta=1$. Then $\phi_{pm}(s)=(\phi_m(s^p))/(\phi_m(s))$. This will only be divisible by p if s^p has order m modulo p, which will happen exactly when s has order m modulo p. In that case, the p-part of $\phi_m(s^p)$ will equal the p-part of $(s^p)^m-1=s^{pm}-1$, which equals the p-part of $p(s^m-1)$ (by Lemma 2.1), as long as $p>2$. And the p-part of $\phi_m(s)$ equals the p-part of s^m-1, so the p-part of $(\phi_m(s^p))/(\phi_m(s))$ will be exactly p. In the case where $p=2$, we will have $m=1$ and $n=2$; we are looking for solutions of $\phi_2(x)\equiv 0 \pmod 2$. In other words, we want to find all values of s where $s+1$ is even; so s must be odd, and the order of s modulo p is $m=1$.

Finally, assume $n = p^\beta m$, and $\beta > 1$. Then $\phi_n(s) = \phi_{pm}(s^{p^{\beta-1}})$. If $p \neq 2$, then by the reasoning above, $\phi_{pm}(s^{p^{\beta-1}})$ will be divisible by p exactly when $s^{p^{\beta-1}}$ has order m modulo p, which will happen exactly when s has order m modulo p. And if that is true, then by the reasoning above, the p-part of $\phi_{pm}(s^{p^{\beta-1}})$ will be exactly p. If $p = 2$, then $m = 1$; $\phi_2(s^{2^{\beta-1}})$ is divisible by 2 exactly when s has order 1 modulo 2 (i.e. when s is odd). And in that case, the 2-part of $\phi_2(s^{2^{\beta-1}}) = s^{2^{\beta-1}} + 1$ will be exactly 2, since $s^{2^{\beta-1}} \equiv 1 \pmod 4$. That completes the proof. □

Next, it will be convenient to have a result similar to that in Lemma 2.1, where the p-part of $s^n + 1$ is compared to the p-part of $s + 1$.

Lemma 2.4. *Let p be a prime, and let s, n be natural numbers where $p|(s+1)$.*

1. *If n is odd, then $p^\alpha \| (s^n + 1)$ iff $p^\alpha \| (n(s+1))$.*
2. *If n is even, then p divides $s^n + 1$ iff $p = 2$, in which case $2^1 \| (s^n + 1)$.*

Proof. 1. If n is odd, then since $(s+1)|(s^n+1)$, p will divide $s^n + 1$. Assume that $p \geqslant 3$; then p does not divide $s^n - 1$. So $p^\alpha \| (s^n + 1)$ iff $p^\alpha \| (s^n + 1)(s^n - 1) = (s^{2n} - 1)$. By Lemma 2.1, this last statement holds iff $p^\alpha \| (n(s^2 - 1))$ (since p divides $s^2 - 1$), which is true iff $p^\alpha \| (n(s+1))$ (since p does not divide $s - 1$).

Now assume that $p = 2$ (so s is odd). If $s \equiv 3 \pmod 4$, then $2^1 \| (s^n - 1)$. Thus, $2^\alpha \| (s^n + 1)$ iff $2^{\alpha+1} \| (s^n + 1)(s^n - 1) = s^{2n} - 1$. Since p divides $s - 1$, Lemma 2.1 shows that the preceding statement is true iff $2^{\alpha+1} \| (2n(s+1))$; that is, exactly when $2^\alpha \| (n(s+1))$. If $s \equiv 1 \pmod 4$, then we have $2^1 \| (s^n + 1)$ and $2^1 \| (n(s+1))$. Either way, the 2-part of $s^n + 1$ equals the 2-part of $n(s+1)$.

2. If n is even, then since p divides $s^2 - 1$, p divides $s^n - 1$ as well. So if $p \geqslant 3$, p does not divide $s^n + 1$. If $p = 2$, then s is odd, and $s^n \equiv 1 \pmod 4$. So $2^1 \| (s^n + 1)$. □

Lemma 2.5. *Let u and b be natural numbers $u \geqslant 2$, let $s = u^b$, and let p be an odd prime. Then if $p^\alpha \| (s^m \pm 1)$ (where $\alpha \geqslant 1$), then $p^\alpha \| b_p(s^{m/b_p} \pm 1)$.*

Proof. For convenience, we will let $v = s^{1/b_p}$. Assume $b_p > 1$; otherwise, the conclusion is trivial.

First, assume that $p^\alpha \| (s^m - 1)$. Since $p|s^m - 1 = v^{mb_p} - 1$, we have $o_p(v)|mb_p$. But we also have $o_p(v)|p - 1$, so $o_p(v)|(mb_p, p-1) = (m, p-1)$. That is, we have $p|v^m - 1$. So by Lemma 2.1, $p^\alpha \| v^{mb_p} - 1$ iff $p^\alpha \| b_p(v^m - 1)$.

Now, assume $p^\alpha \| (s^m + 1)$. The proof of this case is similar. Since $p|s^m + 1$, we have $p|s^{2m} - 1 = v^{2mb_p} - 1$. We thus have $o_p(v)|2mb_p$, but $o_p(v)|p - 1$ also. So $o_p(v)|(2mb_p, p-1) = (2m, p-1)$; we have $p|v^{2m} - 1 = (v^m + 1)(v^m - 1)$. We cannot have $p|v^m - 1$, as then $p|v^{mb_p} - 1 = s^m - 1$, and no odd prime can divide $s^m - 1$ and $s^m + 1$. So $p|v^m + 1$. Then by Lemma 2.4, $p^\alpha \| v^{mb_p} + 1$ iff $p^\alpha \| b_p(v^m + 1)$. □

The final preliminary lemma gives the possible orders of elements of $GL_n(u^c)$ (u prime), where the order must be itself a power of u.

Lemma 2.6. *If $g_r \in GL_n(s)$, where g_r is of order r, and both r and s are powers of the same prime u, then $r < nu$. (Thus, since r is a power of u, we have $r \leqslant (n-1)u$.)*

Proof. We have $(g_r - 1)^n = 0$ (where 1 is the identity matrix, and 0 is the zero matrix), since $g_r \in GL_n(s)$. Let k be the smallest natural number where $(g_r - 1)^k = 0$; then $k \leqslant n$. If $k \leqslant r/u$, then we have $(g_r - 1)^{r/u} = g_r^{r/u} - 1 = 0$. So $g_r^{r/u}$ is the identity, and g_r has order at most r/u, a contradiction. So $k > r/u$, and we thus have $r/u < n$, or $r < nu$. □

3. Proof of main theorem

3.1. Alternating groups

Assume first that $S = A_n$ for some $n \geqslant 5$. Say V is a deleted permutation module. In that case, $d = n-2$ if $p|n$, else $d = n-1$. There must be a prime r where $\lceil n/2 \rceil \leqslant r \leqslant n$ (Bertrand's postulate); this r satisfies $r > d/3$, and there is an element of order r in A_n, hence in G. So the deleted permutation modules arise for all $n \geqslant 5$. (In fact, if r is any prime power where $d/3 < r \leqslant n$, then there must be an element of order r in A_n unless r is a power of 2 and $r = n-1$ or n. In that case, to have an element of order r in G, G must contain S_n.) We will henceforth assume that V is not a deleted permutation module.

If $n \neq 6$, then $\mathrm{Aut}(S) = S_n$, and there is an element of order r in $\mathrm{Aut}(S)$ exactly when $r \leqslant n$. If $n = 6$, there is an element of prime power order r in $\mathrm{Aut}(S)$ if $r \leqslant 5$ or $r = 8$. Let n_0 be the largest prime power less than or equal to n, assuming $n \neq 6$; for $n = 6$, let $n_0 = 8$. We then have $d/3 < r \leqslant n_0$, so $d \leqslant 3n_0 - 1$. From that bound, p. 33 of [13] shows that V must be a deleted permutation module if $n \geqslant 17$. So we can assume that $n \leqslant 16$.

Consider first the case where G' is a proper cover of A_n. We have $G' \cong x \cdot A_n$ for $x \in \{2, 3, 6\}$ if n is 6 or 7, and $G' \cong 2 \cdot A_n$ otherwise. If $n \geqslant 9$, we have $d \geqslant n-2$ from Proposition 5.3.7(i) of [11]. From Proposition 5.3.6 of [11], d is divisible by $2^{\lfloor (n-s-1)/2 \rfloor}$ where s is the number of ones in the binary representation of n. Since $n-2 \leqslant d \leqslant 3n_0 - 1$, we get these possibilities for d: $d = 32$ and $11 \leqslant n \leqslant 15$, $d = 24$ and $9 \leqslant n \leqslant 11$, $d = 16$ and $9 \leqslant n \leqslant 13$, or $d = 8$ and n is 9 or 10. From that, [16] and [7] show we get the examples in Table 1 for which $G' \ncong A_n$. (In the case where $n \leqslant 8$, only the bound $d \leqslant 3n_0 - 1$ is relevant.)

Now assume that $G' \cong A_n$. If $n \geqslant 10$, then Proposition 5.3.5 of [11] shows V is a deleted permutation module if $d \leqslant n$. Thus, we may assume $n+1 \leqslant d \leqslant 3n_0 - 1$. If $n \leqslant 9$, we only have the bound $d \leqslant 3n_0 - 1$ to consider. Then [16] and [7] give us the remaining examples in Table 1.

3.2. Sporadic groups

Now say S is a sporadic group. From [1], we obtain the prime powers r which have corresponding elements $g_r \in \mathrm{Aut}(S)$ of order r. The minimal dimensions of nontrivial representations of each group (in any characteristic) are given in [9]. From that information, and the fact that $r > d/3$ (and $r > 2$), we obtain these possibilities for the pair $(S; r)$:

- Mathieu groups: $(M_{11}; 3, 4, 5, 8, 11)$, $(M_{12}; 3, 4, 5, 8, 11)$, $(M_{22}; 3, 4, 5, 7, 8, 11)$, $(M_{23}, M_{24}; 4, 5, 7, 8, 11, 23)$,
- Janko groups: $(J_1; 3, 5, 7, 11, 19)$, $(J_2; 3, 4, 5, 7, 8)$, $(J_3; 4, 5, 8, 9, 17, 19)$, $(J_4; 43)$,
- Conway groups: $(Co_1; 9, 11, 13, 16, 23)$, $(Co_2; 8, 9, 11, 16, 23)$, $(Co_3; 8, 9, 11, 23)$,
- other sporadic groups: $(HS; 7, 8, 11)$, $(McL; 8, 9, 11)$, $(He; 17)$, $(Ru; 13, 16, 29)$, $(Suz; 5, 7, 8, 9, 11, 13, 16)$, $(O'N; 16, 19, 31)$, $(Fi_{22}; 11, 13, 16)$, $(Ly; 67)$.

From those possibilities, and given that $d \leqslant 3r - 1$, [7] can be used to find the possibilities listed in Table 2.

3.3. Cross characteristic Lie groups – individual cases

Now, assume that S is a Lie type group in cross characteristic. The Landazuri–Seitz bounds found in Theorem 5.3.9 of [11] give a lower bound $d_{\min}$ for d depending on the group S. Also, upper bounds $r_{\max}$ on r were found in [2]. (Most values of $r_{\max}$ are identical to those in [5], where r is required to be prime.) Since $r > d/3$, we can eliminate all groups for which $r_{\max} \leqslant d_{\min}/3$. Such families are listed in Table 6.

There are several individual Lie groups which fall into one of the families mentioned in Table 6, but for which we do not have $r_{\max} \leqslant d_{\min}/3$. They are listed in Table 7; the upper bounds $r_{\max}$ on r come from [1], while the lower bounds $d_{\min}$ now come from [7]. From these bounds, [1] and [7] can

Table 6
Lie groups S where $r_{\max} \leqslant d_{\min}/3$.

S	$d_{\min}$	$r_{\max}$	Constraints
$E_8(s)$	$s^{27}(s^2-1)$	$s^8+s^7-s^5-s^4-s^3+s+1$	
$E_7(s)$	$s^{15}(s^2-1)$	$(s^7-1)/(s-1)$	
$E_6(s)$	$s^9(s^2-1)$	s^6+s^3+1	
${}^2E_6(s)$	$s^9(s^2-1)$	s^6-s^3+1	
$F_4(s)$	$s^6(s^2-1)$	s^4+1	s odd
	$s^7(s^3-1)(s-1)/2$	s^4+1	s even, $s \geqslant 4$
${}^2F_4(s)$	$s^4(s-1)(\sqrt{s/2})$	$s^2+\sqrt{2s^3}+s+\sqrt{2s}+1$	$s=2^{2m+1} \geqslant 8$
${}^3D_4(s)$	$s^3(s^2-1)$	s^4-s^2+1	$s \geqslant 4$
$G_2(s)$	$s(s^2-1)$	s^2+s+1	$s \geqslant 5$
${}^2G_2(s)$	$s(s-1)$	$s+\sqrt{3s}+1$	$s=3^{2m+1} \geqslant 27$
${}^2B_2(s)$	$(s-1)(\sqrt{s/2})$	$s+\sqrt{2s}+1$	$s=2^{2m+1} \geqslant 32$
$\Omega_{2n+1}(s)$, s odd	$s^{2(n-1)}-1$	$(s^n+1)/2$	$n \geqslant 3$, $s>5$
	$s^{n-1}(s^{n-1}-1)$	$(s^n+1)/2$	$n \geqslant 3$, $s=3$ or 5, $(n;s) \neq (3;3)$
$P\Omega^+_{2n}(s)$	$(s^{n-2}+1)(s^{n-1}-1)$	$(s^n-1)/(s-1)$	$n \geqslant 4$, $s \neq 2,3,5$
	$s^{n-2}(s^{n-1}-1)$	$(s^n-1)/(s-1)$	$n \geqslant 4$, $s=2,3,5$, $(n;s) \neq (4;2), (5;3)$
	2160	128	$n=5$, $s=3$
$P\Omega^-_{2n}(s)$	$(s^{n-2}-1)(s^{n-1}+1)$	$(s^n+1)/(4,s^n+1)$	$n \geqslant 4$, $(n;s) \neq (4;2), (5;3)$
	2132	128	$n=5$, $s=3$
$PSp_{2n}(s)$	$s^{n-1}(s^{n-1}-1)(s-1)/2$	s^n+1	$n \geqslant 2$, s even, $(n;s) \neq (2;4), (3;2), (4;2)$
$U_n(s)$	$(s^n-1)/(s+1)$	$(s^{n-1}+1)/(s+1)$	$n \geqslant 6$, n even, $s \neq 2,3$
	$(s^4-1)/(s+1)$	s^2+1	$n=4$, $s \neq 2,3,5,7,9$
	104	32	$n=4$, $s=5$
	300	64	$n=4$, $s=7$
	656	128	$n=4$, $s=9$

Table 7
Individual Lie groups S where $r_{\max} > d_{\min}/3$.

S	$d_{\min}$	$r_{\max}$
$F_4(2)$	52	32
${}^2F_4(2)'$	26	16
${}^3D_4(2)$	25	13
$G_2(3)$	14	13
$G_2(4)$	12	16
${}^2B_2(8)$	8	13
$\Omega_7(3)$	27	13
$P\Omega^+_8(2)$	8	9
$P\Omega^-_8(2)$	33	17
$PSp_6(2)$	7	9
$PSp_8(2)$	35	17
$PSp_4(4)$	18	17
$U_4(2) \cong PSp_4(3)$	4	9
$U_4(3)$	6	9

be used to find the possible values for r and d listed in Table 3 and Table 4. (To simplify the necessary arguments for the upcoming infinite families, we include the groups $U_4(2)$ and $U_4(3)$ here.)

One individual group still needs to be considered: $S = {}^3D_4(3)$ (which does not appear in [1]). In this case, the outer automorphism group of S has order 3; so if r is not the order of an element of S, then $t=3$. We have ${}^3D_4(3) \leqslant P\Omega_8(27)$, so by Lemma 2.6, every 3-element of S has order less than $8(3)=24$; so $r \leqslant 3(9)=27$, contradicting $d \geqslant s^3(s^2-1)=216$ (this bound coming from [11]). So r must be the order of an element of S; we must have $r \leqslant (s^4-s^2+1)=73$. Thus, $216 \leqslant d \leqslant 218$, and [7] shows we can only have $d=218$, $p=2$ or 73.

Table 8
Values that r_i, r_d, r_f, and r_g must divide, for each Lie group S.

S	r_i	r_d	r_f	r_g
$L_n(s)$, $n \geqslant 2$	$s^m - 1$, $m \leqslant n-2$ $(s^{n-1}-1)/(n, s-1)$ $(s^n-1)/(s-1)(n, s-1)$	$(n, s-1)$	b	2 $(n>2)$ 1 $(n=2)$
$PSp_{2n}(s)$, $n \geqslant 2$, s odd	$s^m \pm 1$, $m < n$ $(s^n \pm 1)/2$	2	b	1
$U_n(s)$, $n \geqslant 3$	$s^m - (-1)^m$, $m \leqslant n-2$ $(s^{n-1}-(-1)^{n-1})/(n, s+1)$ $(s^n-(-1)^n)/(s+1)(n, s+1)$	$(n, s+1)$	$2b$	1

Having dealt with these individual groups, we still must consider the following four families of groups not mentioned in Table 6:

- $PSp_{2n}(s)$, where s is odd and $n \geqslant 2$,
- $U_n(s)$, where $n \geqslant 3$ is odd,
- $U_n(s)$, where $n \geqslant 6$ is even and $s = 2$ or 3, and
- $L_n(s)$, where $n \geqslant 2$.

To handle these, we will first mention some facts about elements of simple groups of Lie type. Given such a group S, and given any element $g_r \in \mathrm{Aut}(S)$, we have $g_r = h_i h_d h_f h_g$, where h_i is an inner automorphism, h_d is a diagonal automorphism, h_f is a field automorphism, and h_g is a graph automorphism. (If S is twisted, then h_g must be the identity.) In all cases, h_f and h_g commute with each other. These facts are proven, for example, in Section 2.5 of [3].

We will let r_f be the order of h_f, r_g be the order of h_g, and r_{fg} be the order of $h_f h_g$. For the infinite families we will consider, we always have $r_{fg} = \mathrm{lcm}(r_f, r_g)$. If the order of g_r is r, then we can say that $r = r_i r_d r_{fg}$, where r_i is the order of an element of S, and r_d is the order of a diagonal automorphism. Where appropriate, we'll let $\widetilde{r} = r_i r_d$; $\widetilde{r}$ is the order of $h = g_r^{r_{fg}}$, which is the product of an inner automorphism and a diagonal automorphism.

Table 8 gives the possible values of r_i, r_d, r_f, and r_g for each of our remaining infinite families. In each case, r_i, r_d, r_f, and r_g must divide one of the values given. The possible values for r_d, r_f, and r_g for each of our groups are given in [3]; we assume that $s = u^b$, where u is prime. The values for r_i are given in [12]; they assume that r_i is a power of a prime other than u.

Finally, we have the following results about the possible values of $\widetilde{r}$, given the value of r_f. The results in Lemma 3.1 were proven in [2]. Note: following the notation in [3], we will denote by $\mathrm{Inndiag}(S)$ the subgroup of $\mathrm{Aut}(S)$ consisting of all products of inner and diagonal automorphisms (i.e. all elements g_r where $r_{fg} = 1$). Also, for simplicity, $X_m(s)$ is used to represent a general untwisted Lie group; X can represent A, B, C, D, E, F, or G.

Lemma 3.1. (a) *If $S = X_m(s)$ is an untwisted group, and $r_g = 1$, then $\widetilde{r}$ is the order of an element of $\mathrm{Inndiag}(X_m(s^{1/r_f}))$.*

(b) *If $S = X_m(s)$ is an untwisted group, and $r_g = 2$, then $\widetilde{r}$ is the order of an element of $\mathrm{Inndiag}({}^2X_m(s^{1/r_f}))$. If $S = D_4(s)$ and $r_g = 3$, then $\widetilde{r}$ is the order of an element of $\mathrm{Inndiag}({}^3D_4(s^{1/r_f}))$. (In the case where S is of type B_2, F_4, or G_2, and $r_g = 2$, we must have $r_f = b_2$.)*

(c) *Assume $S = {}^2X_m(s)$ is a twisted group of type ${}^2A_l$, ${}^2D_l$, or type ${}^2E_6$. If r_f is even, then $\widetilde{r}$ is the order of an element of $\mathrm{Inndiag}({}^2X_m(s^{2/r_f}))$. If r_f is odd, then $\widetilde{r}$ is the order of an element of $\mathrm{Inndiag}({}^2X_m(s^{1/r_f}))$. (In both cases, $\widetilde{r}$ is also the order of an element of $\mathrm{Inndiag}(X_m(s^{2/r_f}))$.)*

Part (a) is proven as follows (and the other parts are similar): let $\overline{S}$ be the algebraic group corresponding to S, and let φ be the automorphism of $\overline{S}$ denoted by φ_u on pg. 29 of [3]. (That is,

$\varphi(x_\alpha(v)) = x_\alpha(v^u)$, for all roots α and for all v in the algebraic closure of $GF(u)$.) Then Inndiag(S) consists of exactly those elements of $\overline{S}$ fixed by φ^b. We have $h_f = \varphi^c$ for some $c < b$; we have $r_f = b/(b,c)$. It can be shown that h (an element of Inndiag(S)) is conjugate to another element $h' \in$ Inndiag(S) that is fixed by φ^c. But since h' is also fixed by φ^b (as all elements of Inndiag(S) are), h' is fixed by $\varphi^{(b,c)}$. So h' is an element of Inndiag$(X_m(u^{(b,c)})) =$ Inndiag$(X_m(s^{1/r_f}))$. That completes the proof, since the order of both h and h' is $\widetilde{r}$.

Now to consider the remaining infinite families of Lie groups. For each family, the possible groups S and the possible values of r will be determined first; the values of d will be determined last.

3.4. $S = PSp_{2n}(s)$, s odd

Since $S = PSp_4(3) \cong U_4(2)$ was already considered, assume that $(n; s) \neq (2; 3)$. We have $r_d|2$, $r_f|b$, and $r_g = 1$. From [4], $d \geqslant (s^n - 1)/2$, so we must have $r > (s^n - 1)/6$.

Assume $r_f > 1$. Then we have $r \leqslant r_f(s^{n/r_f} + 1)/2 \leqslant (s^n - 1)/6$, unless $n \leqslant 3$ and $s^{1/r_f} = 3$. In that case, we have $r \leqslant 9r_f$, which cannot exceed $(s^n - 1)/6$ unless $s = 9$ and $n = r_f = 2$. In that case, r is a power of 2, so $r \leqslant 16$; to have $r > (s^n - 1)/6$, we must in fact have $r = 16$.

Hereafter, we may assume $r_f = 1$. Say $t = u$. Then $r_d = 1$, and Lemma 2.6 shows that $r = r_i < 2nu$. We thus cannot have $r > (s^n - 1)/6$ unless $n = 3$ and $s = 3$ or 5. If $s = 3$, then $d_{\min} = 13$, and [1] shows we can have $r = 9$. If $s = 5$, then $d_{\min} = 62$, and we must have $r = 25$.

Now say $t \neq u$; we have $r_i|(s^m \pm 1)$ for some $m \leqslant n$, and if $m = n$, then $r_i|(s^n \pm 1)/2$. Assume $t = 2$. Then by Lemmas 2.1 and 2.4, $r_i|(m(s \pm 1))$; if $m = n$, then $r_i|(n/2)(s \pm 1)$. So $r = r_d r_i \leqslant 2(n-1)(s+1)$. If $n \geqslant 3$, we can only have $2(n-1)(s+1) > (s^n - 1)/6$ when $s = 3$ and $n = 3$ or 4. From [1], we can have $r = 8$ when $S = PSp_6(3)$; if $S = PSp_8(3)$, we can only have $r > (s^n - 1)/6$ if $r = 16$. If $n = 2$, then $r_i|(s \pm 1)$ or $r_i|(s^2 \pm 1)/2$; in all cases, r_i can be no larger than the 2-part of $s - 1$ or $s + 1$. So $r = r_d r_i \leqslant 2(s+1)$, and we can have $2(s+1) > (s^2 - 1)/6$ only when $s \leqslant 11$. From [1], we may have $r = 8$ when $s = 5$. If $s = 7$ or 9, then to have $r > (s^2 - 1)/6 \geqslant 8$, we must have $r = 16$. And if $s = 11$, then since $r_i|(s \pm 1)$, we have $r_i \leqslant 4$, so $r \leqslant 2r_i \leqslant 8 < (s^2 - 1)/6$. So we cannot have $s = 11$.

Now assume $t \neq u$ and $t \neq 2$; then $r_d = 1$, so $r = r_i$. Say $r_i|(s^m - 1)$ for some $m \leqslant n$. If $t|(s - 1)$, then since $t \neq 2$, $s - 1$ is not a power of 2. Further, we have $r_i|(m(s-1)) \leqslant n(s-1)$; given that $s - 1$ is not a power of 2, we can only have $n(s-1) > (s^n - 1)/6$ when $n = 2$ and $s = 7$ or $s = 11$. But if $n = 2$, we have $r_i|(2(s-1))$, and since $t \neq 2$, we have $r_i|s - 1 < (s^n - 1)/6$. So t cannot divide $s - 1$; thus, we must have $r_i|(s^m - 1)/(s - 1)$. That is enough to show that $r = r_i \leqslant (s^n - 1)/6$ unless $m = n$ and $s = 3$ or 5. If $s = 3$, then we must have $r = (3^n - 1)/2$; $r = (3^n - 1)/4$ is a prime power only when $n = 2$, and the group $PSp_4(3)$ has already been considered. And if $s = 5$, we must have $r = (5^n - 1)/4$.

Now say $r_i|(s^m + 1)$ for some $m \leqslant n$; since $s^m + 1$ is even and $t \neq 2$, we have $r_i|(s^m + 1)/2$. That suffices to show that $r = r_i \leqslant (s^n - 1)/6$ unless $m = n - 1$ or n. In the case where $m = n - 1$, r can only be sufficiently large if $s = 3$; we must have $r = (3^{n-1} + 1)/2$. If $m = n$, then we must have $r = (s^n + 1)/2i$, where $1 \leqslant i \leqslant 3$. (If $i = 3$, then $r = (s^n + 1)/6$ can only be a prime power when $s = 5$.)

Finally, what values can d take if $S = PSp_{2n}(s)$ for s odd? From Theorem 2.1 of [4], if d is not $(s^n \pm 1)/2$, then $d \geqslant (s^n - 1)(s^n - s)/2(s+1)$. This contradicts $r > d/3$ in all cases mentioned above (the case where $S = PSp_4(3)$ does arise, but it has already been considered). So we must have $d = (s^n \pm 1)/2$ in all cases.

3.5. $S = U_n(s)$, $n \geqslant 3$ odd

Since $U_3(2)$ is not simple, we assume that $(n; s) \neq (3; 2)$. We have $r_d|(n, s+1)$; since n is odd, so is r_d. Also, $r_g = 1$, and $r_f|(2b)$. From [4], we have $d \geqslant (s^n - s)/(s+1)$, thus $r > (s^n - s)/3(s+1)$.

Assume first that $t = u$; then $\widetilde{r} = r_i < nu$ from Lemma 2.6. If $u \neq 2$, then $r \leqslant br_i < bnu$. We will have $bnu < (s^n - s)/3(s+1)$ if $n \geqslant 5$; if $n = 3$, then since $r_i < nu = 3u$ and u is odd, we have $r_i \leqslant u$. So $r \leqslant ub$ in that case, and we can only have $ub > (s^3 - s)/3(s+1)$ if $s = 3$ (then we must have $r = 3$). If $u = 2$, then $r \leqslant 2b_2 r_i < 4b_2 n$; thus $r \leqslant 4b_2(n-1)$. We will have $4b_2(n-1) < (s^n - s)/3(s+1)$ unless we have $(n; s) = (7; 2)$, $(5; 2)$, or $(3; 4)$. In the first two cases, we have $r \leqslant 24$; r is a power of 2, so $r \leqslant 16$. From [1], we can have $r \in \{4, 8, 16\}$ when $S = U_5(2)$, we can only have $r = 16$ when $S = U_7(2)$, and we can have $r \in \{8, 16\}$ when $S = U_3(4)$.

Now, say $t \neq u$. We have $r_i|(s^m-(-1)^m)$, where $1 \leqslant m \leqslant n$. If $m = n-1$, then $r_i|(s^{n-1}-1)/(n, s+1)$; if $m = n$, then $r_i|(s^n+1)/(s+1)(n, s+1)$. Assume first that $t = 2$ (then s is odd); since r_d is odd, $r_d = 1$. If $r_i|(s^m+1)$ for m odd, then by Lemma 2.4, $r_i|(m(s+1))$, hence $r_i|(s+1)$. If $r_i|(s^m-1)$ for m even, then by Lemma 2.1, $r_i|(m(s\pm 1))$. So $r_i \leqslant (n-1)(s+1)$ regardless, and $r \leqslant 2b_2(n-1)(s+1)$. We only have $2b_2(n-1)(s+1) > (s^n-s)/3(s+1)$ when $n = 5$ and $s = 3$, or $n = 3$ and either $s \leqslant 13$ or $s = 25$. If $S = U_5(3)$, r is sufficiently large only if $r = 32$. If $n = 3$ and $s \leqslant 11$, then [1] shows that we have sufficiently large values of r when $s = 3$ ($r = 4$ or 8), $s = 5$ ($r = 8$), or $s = 7$ ($r = 16$). Say $s = 13$; we already showed that $r_i|(2(s\pm 1))$, so $r_i \leqslant 8$ and $r \leqslant 16$, which is too small. If $s = 25$, then again, $r_i|(2(s\pm 1))$; so $r_i \leqslant 16$, and $r \leqslant 64$, again too small. So if $t = 2$, then $S = U_5(3)$, $U_3(3)$, $U_3(5)$, or $U_3(7)$.

We may now assume that $t \neq 2$; then $r_f|b$. Assume that $r_d > 1$; then $t|(n, s+1)$. If $r_i|(s^m+1)$ for $m \leqslant n$ odd, then Lemma 2.4 shows that since $t|(s+1)$, we have $r_i|(m(s+1))$. Note: if $m = n$, then we have $r_i|(n(s+1))/((s+1)(n, s+1)) = n/(n, s+1)$; we thus have $r_i \leqslant n$. So for any m odd, we have $r_i \leqslant (n-2)(s+1)$. If $r_i|(s^m-1)$ for $m \leqslant n$ even, then Lemma 2.1 shows that since $t|(s^2-1)$, $r_i|(m/2)(s^2-1)$. But since t does not divide $s-1$, we have $r_i|(m/2)(s+1)$. Thus, we have $r_i \leqslant (n-2)(s+1)$ for any value of m, and $r \leqslant b_t(n, s+1)(n-2)(s+1)$. Given that bound, r can only be sufficiently large if $(n; s) = (9; 2), (5; 4), (3; 5, 8)$. If $n = 3$ (and $t = 3$), then [1] shows that $r = 3$ if $s = 5$, and $r \leqslant 9$ if $s = 8$; both are too small. If $(n; s) = (5; 4)$, then $t = 5$. We have $r_i \leqslant (n-2)(s+1) = 15$, so $r_i \leqslant 5$, and $r \leqslant 25$, which is too small. And if $(n; s) = (9; 2)$, then $t = 3$. We have $r_i \leqslant (n-2)(s+1) = 21$, so $r_i \leqslant 9$, and $r \leqslant 27$, again too small. So no cases where $r_d > 1$ arise.

Next, assume $r_d = 1$ and $r_f > 1$. If $r_i|(s^m-(-1)^m)$ for $m \leqslant n$, then by Lemma 2.5, $r_i|(b_t(s^{m/b_t}-(-1)^m))$. So $r \leqslant b_t r_i \leqslant b_t^2(s^{n/b_t}+1)$, and that suffices to show that r is too small unless $t = n = 3$ and $s = 8$. (We exclude the case where $n = 3$ and $s = 27$, since then we would have $t = u = 3$.) We would need to have $r = 27$, but [1] shows this is impossible.

We may now assume that $r_d = r_f = 1$, so that $r = r_i$. We have $r_i|(s^m-(-1)^m)$ for some $m \leqslant n$. We cannot have $m \leqslant n-4$, since $s^{n-4}+1 \leqslant (s^n-s)/3(s+1)$ in all cases. If $m = n-3$ ($n \geqslant 5$), then $r|(s^{n-3}-1) = (s^{(n-3)/2}-1)(s^{(n-3)/2}+1)$. Since $t \neq 2$, we have $r_i \leqslant s^{(n-3)/2}+1 \leqslant s^{n-4}+1$, and again r is too small. If $m = n-2$, we have $s^{n-2}+1 > (s^n-s)/3(s+1)$ exactly when $s = 2$ or 3. If $s = 3$, then r can only be large enough if $r = 3^{n-2}+1$, which can only be a prime power when $n = 3$ (then $r = 4$). If $s = 2$, then $n \geqslant 5$. We then have $(2^{n-2}+1)/3 \leqslant (2^n-2)/9$, so we must have $r = 2^{n-2}+1$, which is a prime power only when $n = 5$ (then $r = 9$).

If $m = n-1$, then $r_i|(s^{n-1}-1) = (s^{(n-1)/2}-1)(s^{(n-1)/2}+1)$; since $t \neq 2$, we have $r_i \leqslant s^{(n-1)/2}+1$. We thus can only have $r > (s^n-s)/3(s+1)$ when $(n; s) = (5; 2)$ (we must have $r = 5$) or $(n; s) = (3; 4)$ (then $r|(s^2-1) = 15$, so $r = 5$). Finally, if $m = n$, then $r = r_i|(s^n+1)/(s+1)$; we have $r = (s^n+1)/j(s+1)$ for some j. Clearly, we will then have $r > (s^n-s)/3(s+1)$ if $1 \leqslant j \leqslant 3$. But r will not be an integer if $j = 2$, and if $j = 3$, then $r = (s^n+1)/3(s+1)$ can only be a prime power when $n = 3$. If $j > 3$, then we can only have $r > (s^n-s)/3(s+1)$ when $j = 4$ and $s = 2$. But then r is not an integer. So we either have $n = j = 3$, or $j = 1$.

Finally, what values may d take when $S = U_n(s)$, for $n \geqslant 3$ odd? Say $n \geqslant 5$. From [4], if we do not have $d = (s^n-s)/(s+1)$ nor $d = (s^n+1)/(s+1)$, then we have $d \geqslant (s^n+1)(s^{n-1}-s^2)/(s^2-1)(s+1)-1$. This contradicts $r > d/3$ in all cases mentioned above, except for where $S = PSU_5(2)$ and $r = 16$. In that case, we need $d \leqslant 47$; [7] shows that, besides the Weil modules ($d = 10$ and $p \neq 2$, or $d = 11$ and $p \geqslant 5$), we may have $d = 43$ ($p = 5$) or $d = 44$ ($p \neq 2, 5$).

In the case where $n = 3$, Theorem 16 from [8] shows that if we do not have $d = (s^3-s)/(s+1)$ nor $d = (s^3+1)/(s+1)$, then $d \geqslant (s-1)(s^2+3s+2)/6$ if $3|(s+1)$, and $d \geqslant (2s^3-s^2+2s-3)/3$ if $s > 3$ and 3 does not divide $s+1$. (If $n = s = 3$, then [7] shows that we have $d \geqslant 14$.) That contradicts $r > d/3$ in all cases mentioned above, except for the following: $s = 3$ and $r = 7$ or 8, $s \in \{5, 8, 11\}$ and $r = (s^n+1)/(s+1)$, or $s = 5$ and $r = (s^n+1)/2(s+1)$. We only need consider the case where $S = U_3(3)$ and $r = 7$ or 8, since the other cases don't produce prime power values of r. We must have $d \leqslant 23$, and [7] shows we may have $d = 14$ (any $p \neq 3$ is possible) or $d = 21$ (then $p \geqslant 5$). So except when $S = U_3(3)$ or $U_5(2)$, we must have $d = (s^n-s)/(s+1)$ or $d = (s^n+1)/(s+1)$.

3.6. $S = U_n(s)$, $n \geqslant 6$ even, $s = 2$ or 3

We have $r_d|(n, s+1)$, $r_g = 1$, and $r_f|2$. Also, we have $r \leqslant r_{\max} = (s^{n-1}+1)/(s+1)$ unless $n = 6$ (we may have $r = 16$ when $s = 2$, or $r = 64$ when $s = 3$), and $d \geqslant d_{\min} = (s^n - 1)/(s+1)$.

Assume first that $s = 3$. Then unless $n = 6$, we have $d_{\min} = 3r_{\max} - 1$, so the only possibility is that $d = d_{\min} = (3^n - 1)/4$ and $r = r_{\max} = (3^{n-1}+1)/4$. (We must then have $n-1$ prime, in order to have r be a prime power.) If $n = 6$, then $r = 61$ or $r = 64$; we then have $d \leqslant 191$, and [7] shows that we must have $d = 182$ or $d = 183$.

Now say $s = 2$. Consider the case where $t|(s+1)$ (i.e. $t = 3$). Then $r_d|(n, 3)$, and $r_f = 1$. If $r_i|(2^m+1)$ for $m < n$ odd, then by Lemma 2.4, $r_i|(m(2+1)) = 3m$. If $r_i|(2^m - 1) = (4)^{m/2} - 1$ for $m \leqslant n$ even, then since $t|(s^2 - 1)$, Lemma 2.1 shows that $r_i|(m/2)(4-1) = (3m/2)$. In all cases, we have $r_i \leqslant 3(n-1)$, so $r \leqslant 3(n, 3)(n-1)$; we have $3(n, 3)(n-1) \leqslant d/3$ unless $n = 6$ or 8. But if $n = 8$, then $r \leqslant 21$; thus $r \leqslant 9 < d/3$. So we may only have $n = 6$. We then have $d \geqslant 21$, thus $r \geqslant 8$; [1] shows we must have $r = 9$.

Now assume that $t \neq 3$; then $r_d = 1$. If $t = u = 2$, then $\widetilde{r} = r_i < nu$; we thus have $r \leqslant r_f(n-2)u \leqslant 4(n-2)$. That will contradict $r > d/3$ unless $n = 6$; then [1] shows we may have $r = 8$ or $r = 16$. If $t \neq u$, then $r = r_i$, and we must have $r > d_{\min}/3 = (2^n - 1)/9$. We have that r divides $2^m - (-1)^m$ for some m where $2 \leqslant m \leqslant n$; for r to be a sufficiently large prime power, we must have $r = (2^{n-1}+1)/3$ (or $n = 6$ and $r = 9$, but that has already been considered). Here, $n-1$ must be prime.

What values may d take when $S = U_n(s)$ for $n \geqslant 6$ even, and $s = 2$ or 3? Theorem 2.7 of [4] shows that for $n \geqslant 6$, if we do not have a Weil module (i.e. if we do not have $d = (s^n - 1)/(s+1)$ or $d = (s^n + s)/(s+1)$), then we have $d \geqslant [(3^n - 1)(3^{n-1}+1)/32] - 2$ if $s = 3$, and $d \geqslant (2^n - 1)(2^{n-1} - 2)/9$ if $s = 2$. This contradicts $r > d/3$ in all aforementioned cases. Thus, we must always have $d = (s^n - 1)/(s+1)$ or $d = (s^n + s)/(s+1)$.

3.7. $S = L_n(s)$, $n \geqslant 2$

Since the alternating groups were already discussed, and since $L_3(2) \cong L_2(7)$, we may assume that $(n; s) \neq (3; 2), (4; 2)$, and if $n = 2$, then $s \geqslant 7$ and $s \neq 9$. We have $r_d|(n, s-1)$, $r_f|b$, and $r_g|2$; if $n = 2$, then $r_g = 1$. Our primary reference for this case is Theorem 1.1 of [6]; to use it, we will first assume that $n \geqslant 3$ and $(n; s) \neq (3; 4), (4; 3), (6; 2), (6; 3)$.

From the introduction to [6] (p. 117), $d \geqslant ((s^n - 1)/(s-1)) - 2$, so $r \geqslant (s^n - s)/3(s-1)$. Say $t = u$; then $\widetilde{r} = r_i$. Let b' be the u-part of $\operatorname{lcm}\{2, b\}$; then $r_{fg}|b'$, and $r \leqslant b' r_i < b'un$. Thus, $b'un > (s^n - s)/3(s-1)$, which is only possible when $n = 5$, $s = 2$. In that case, $(s^n - s)/3(s-1) = 10$ and $b'un = 20$, so we must have $r = 16$; from [1], there is indeed an element of order 16 in $\operatorname{Aut}(L_5(2))$.

Now say $t \neq u$; then $r_i|(s^m - 1)$ for some $m \leqslant n$. If $m = n-1$, then $r_i|(s^{n-1} - 1)/(n, s-1)$; if $m = n$, then $r_i|(s^n - 1)/(s-1)(n, s-1)$. Assume first that $t = 2$. Again, let b' be the 2-part of $\operatorname{lcm}\{2, b\}$; then $r_{fg}|b'$. If $r_i|(s^m - 1)$, then since $t|(s-1)$, we have $r_i|(m(s \pm 1))$. So $r \leqslant r_{fg} r_d r_i \leqslant b'((n, s-1)_2)n(s+1)$. That suffices to show $r < (s^n - s)/3(s-1)$ if $n \geqslant 5$, so we only need consider what happens when $n = 3$ or 4.

- $n = 4$: Either $r_i|(s-1)$, $r_i|(s^2-1)$ (then $r_i|2(s \pm 1)$), $r_i|(s^3-1)/2$ (then $r_i|(s-1)/2$), or $r_i|(s^4-1)/2(s-1) = (s+1)(s^2+1)/2$ (then $r_i|(s+1)$, since the 2-part of s^2+1 is 2). We thus have $r_i \leqslant 2(s+1)$ regardless, so $r \leqslant 2b'(4, s-1)(s+1)$, and that is less than $(s^4 - s)/3(s-1)$ unless $s = 3$ or 5. The case where $(n; s) = (4; 3)$ will be considered later; if $s = 5$, then [16] shows that since r is a power of 2, we must have $r \leqslant 8 < (s^4 - s)/3(s-1)$. So no possibilities arise here.
- $n = 3$: Either $r_i|(s-1)$, $r_i|(s^2-1)$ (then $r_i|2(s \pm 1)$), or $r_i|(s^3-1)/(s-1) = s^2+s+1$ (then $r_i = 1$). We thus have $r_i \leqslant 2(s+1)$ regardless, so $r \leqslant 2b'(s+1)$. That is less than $(s^3 - s)/3(s-1)$ unless $s \in \{3, 5, 9\}$. From [1], given that r is a power of 2, we have $r \leqslant 8 < (s^3 - s)/3(s-1)$ if $s = 5$, and $r \leqslant 16 < (s^3 - s)/3(s-1)$ if $s = 9$. So we must have $s = 3$; then $r \geqslant (s^3 - s)/3(s-1) = 4$, and from [1], we may have $r = 4$ or $r = 8$.

We may now assume that $t \neq u$ and $t \neq 2$; thus $r_g = 1$, and $r_{fg} = r_f|b$. If $r_f > 1$, then we have $r = r_f \widetilde{r} \leqslant r_f(s^{n/r_f} - 1)/(s^{1/r_f} - 1)$. (The one case where we could have $\widetilde{r} > (s^{n/r_f} - 1)/(s^{1/r_f} - 1)$ is

where $n = 3$, $s^{1/r_f} = 2$, and $\widetilde{r} = 8$; but then $t = u$.) Given that r_f is not a power of u, this shows $r < (s^n - s)/3(s-1)$ in all cases where $n \geqslant 3$. So we may assume that $r_f = 1$, and $r = \widetilde{r}$.

Say $r_d > 1$; then $t|(r_d)|(n, s-1)$, so since $t \geqslant 3$, we have that $(n, s-1)$ is not a power of 2. (So $s \geqslant 4$.) Also, if $r_i|(s^m - 1)$, then by Lemma 2.1, $r_i|(m(s-1))$. So we have $r \leqslant (n, s-1)r_i \leqslant (n, s-1)n(s-1)$. Given that $(n, s-1) > 1$ is not a power of 2, we can only have $(n, s-1)n(s-1) \geqslant (s^n - s)/3(s-1)$ when $n = 3$ and $s \in \{4, 7, 13, 16, 19\}$. If we do have $t = n = 3$, then either $r_i|(s-1)$, $r_i|(s^2-1)/(3, s-1)$ (then $r_i|(s-1)/3$), or $r_i|(s^3-1)/(s-1)(3, s-1)$ (then $r_i|3(s-1)/(s-1)(3, s-1) = 1$). So $r_i|(s-1)$ in all cases, and $r \leqslant (n, s-1)r_i \leqslant 3(s-1)$. We will only have $3(s-1) \geqslant (s^3-s)/3(s-1)$ if $s = 4$, and that case will be considered later.

Finally, we may assume that $r_d = 1$; thus $r = r_i$. If $r_i|(s^m - 1)$ for $m \leqslant n-2$, we have $r_i \leqslant s^{n-2} - 1 < (s^n - s)/3(s-1)$. If $r_i|(s^{n-1} - 1)/(n, s-1)$, we must have $r_i = s^{n-1} - 1$ or $(s^{n-1} - 1)/2$, since $(s^{n-1} - 1)/3 < (s^n - s)/3(s-1)$. For r_i to be a prime power, we must have $r_i = 2^{n-1} - 1$ (i.e. $s = 2$) or $r_i = (3^{n-1} - 1)/2$ (i.e. $s = 3$). Finally, if $r_i|(s^n - 1)/(s-1)(n, s-1)$, we must have $r_i = (s^n - 1)/i(s-1)$ for $1 \leqslant i \leqslant 3$, since if $i \geqslant 4$, then $(s^n - 1)/i(s-1) < (s^n - s)/3(s-1)$. But note that if $i > 1$, then r_i can only be a prime power when $i = n = 3$.

Now, what values of d can we have for these values of r? Since $r \leqslant (s^n - 1)/(s-1)$ in all cases, we have $d \leqslant (3s^n - s - 2)/(s-1)$. That bound is small enough for Theorem 1.1 of [6] to show that we must have $(s^n - 1)/(s-1) - 2 \leqslant d \leqslant (s^n - 1)/(s-1)$, except in the following cases:

- $S = L_4(4), L_4(5), L_4(7)$: These cases do not lead to any prime power r of a form mentioned above.
- $S = L_3(7)$: From above, we must have $r = 19$. Thus $d \leqslant 56$, and that bound is small enough for [6], Theorem 1.1 to apply.
- $S = L_5(2)$: We have $r \leqslant 31$, so we will have $32 \leqslant d \leqslant 92$ for any cases not covered by [6], Theorem 1.1. From [1] and [10], there are no examples.
- $S = L_3(3)$: As $r \leqslant 13$, we want cases where $14 \leqslant d \leqslant 38$. Then [1] and [10] show we can have $d = 16$, $d = 26$, or (if $p \neq 2, 3, 13$) $d = 27$. These are the only cases so far where we can have $d > (s^n - 1)/(s-1)$.

Now, we return to the groups where $n \geqslant 3$ that were not yet considered. If $(n; s) = (6; 3)$, then $r_d|(n, s-1) = 2$, $r_f = 1$, and $r_{fg} = r_g|2$. From Table III of [6], we have $d \geqslant 362$. If $t = u = 3$, then we have $r = r_i < un = 18$, which is too small. So $t \neq u$; we have that $r_i|(s^m - 1) = 3^m - 1$ for $m \leqslant 4$, $r_i|(s^{n-1} - 1)/(n, s-1) = 121$, or $r_i|(s^n - 1)/(s-1)(n, s-1) = 182$. If $t = 2$, then $r_i \leqslant 16$, and $r \leqslant 4r_i \leqslant 64$, which is too small. So $t \neq 2$, and $r = r_i \leqslant 121$. We must in fact have $r = 121$ and $d = 362$; that case is covered by an infinite family in Table 5.

If $(n; s) = (6; 2)$, then $r_d = r_f = 1$, and $r_g|2$. From Table III of [6], $d \geqslant 61$; thus $r \geqslant 21$. If $t = 2$, then $r \leqslant 2r_i < 2un = 24$. Thus $r \leqslant 16$, a contradiction. So $t \neq u$; we have $r_g = 1$, and $r = r_i$. From Section 3.1 of [12], we have $r_i|(s^m - 1) = 2^m - 1$ for $m \leqslant 4$, $r_i|(s^{n-1} - 1)/(n, s-1) = 31$, or $r_i|(s^n - 1)/(s-1)(n, s-1) = 63$. We must have $r = r_i = 31$; thus $d \leqslant 92$. From [6], Table III, we see that we must have $d = 61$ or 62. But that case is already covered by an infinite family in Table 5.

If $(n; s) = (4; 3)$, then $d \geqslant 26$; thus $r \geqslant 9$. From [1], $r = 9$ or 13; thus $d \leqslant 38$. From Table III of [6], we can have $d = 26$ or (if $p = 2$ or 5) $d = 38$. In the latter case, r must be 13. (Only the $d = 26$ case is listed in Table 3, since the $d = 38$ case is covered by an infinite family in Table 5.)

Finally, assume that $(n; s) = (3; 4)$. From [1], $r \in \{2, 3, 4, 5, 7, 8\}$, so $d \leqslant 23$. Thus, we must have $d \in \{4, 6, 8, 10, 12, 15, 16, 19, 20, 21, 22\}$; these are all given in [1] and [10]. All these possibilities are listed in Table 3.

Now we consider the case where $n = 2$: $s \geqslant 7$, $s \neq 9$. We now have $r_g = 1$. From [8], the irreducible representations of $L_2(s)$ have order $(s-1)/2$, $(s+1)/2$ (those two occur if and only if s is odd), $s-1$, s, and $s+1$. Since $d \geqslant (s-1)/2$, we must have $r > (s-1)/6$. (If s is even, then $r > (s-1)/3$.) If $t = u$, then $r_i < nu = 2u$, so $r_i|u$. Since $r_d = 1$ in this case, $r|bu$. In fact, we can show that $r = u$ in most cases; if $r = u^{i+1}$, then u^i is a factor of b, and $d \geqslant (s-1)/2 \geqslant (u^{u^i} - 1)/2$. (If $u = 2$, then $d \geqslant s - 1 \geqslant u^{u^i} - 1$.) If $i \neq 0$ (i.e. if $r > u$), we can only have $3r > d$ if $(r; s) = (8; 16)$ or $(9; 27)$ ([1] shows that both values of r are possible). Besides those cases, we must have $r = u$; we can only have $3r > d$ if $s = u$ (i.e. if s is prime).

Now say $t \neq u$; we can then show that $r|(s \pm 1)$, as follows. Since $\widetilde{r}$ is the order of an element of $\mathrm{Inndiag}(L_2(s^{1/r_f}))$, we have that $\widetilde{r} = r'_d r'_i$, where r'_i and r'_d are orders of inner and diagonal automorphisms of $L_2(s^{1/r_f})$. By Section 3.1 of [12], $r'_i|(s^{1/r_f} \pm 1)/(2, s^{1/r_f} - 1)$. Since $r'_d|(2, s^{1/r_f} - 1)$, we have $\widetilde{r}|(s^{1/r_f} \pm 1)$. We thus have $r|(r_f(s^{1/r_f} \pm 1))$. Lemmas 2.1 and 2.4 then show that $r|(s \pm 1)$, unless $r = r_f$. (If $t = 2$ and $r|(r_f(s^{1/r_f} + 1))$, then we can say $r|(s - 1)$.) But if $r = r_f$, then we have $r_f \geqslant (s-1)/6$, with $r_f \geqslant (s-1)/3$ if s is even. This is only possible if $r = 3$, $s = 8$; but then we have $r|(s + 1)$. So $r|(s \pm 1)$ in all cases.

Since $r|(s \pm 1)$ and $r > d/3 \geqslant (s-1)/6$, we get the infinite families in Table 5. Note the following:

- $r = (s-1)/5$: If s is not prime, then for r to be a prime power, we must have $s = 81$.
- $r = (s-1)/3$: If s is not prime, then for r to be a prime power, $s = 25$ or 49.
- $r = s + 1$: Either r or s will be prime (and the other will be a power of 2) unless $s = 8$, $r = 9$.

References

[1] J.H. Conway, R.T. Curtis, S.P. Norton, R.A. Parker, R.A. Wilson, An ATLAS of Finite Groups, Clarendon Press, Oxford, 1985.
[2] J. DiMuro, On prime power elements of $GL_d(q)$ acting irreducibly on large subspaces, PhD thesis, University of Southern California, 2008.
[3] D. Gorenstein, R. Lyons, R. Solomon, The Classification of the Finite Simple Groups, Number 3, Math. Surveys Monogr., vol. 40, American Mathematical Society, Providence, RI, 1998.
[4] R.M. Guralnick, K. Magaard, J. Saxl, Pham Huu Tiep, Cross characteristic representations of symplectic groups and unitary groups, J. Algebra 257 (2002) 291–347.
[5] R.M. Guralnick, T. Penttila, C.E. Praeger, J. Saxl, Linear groups with orders having certain large prime divisors, Proc. Lond. Math. Soc. 78 (1999) 167–214.
[6] R.M. Guralnick, Pham Huu Tiep, Low-dimensional representations of special linear groups in cross characteristics, Proc. Lond. Math. Soc. 78 (1999) 116–138.
[7] G. Hiss, G. Malle, Corrigenda: Low-dimensional representations of quasi-simple groups, LMS J. Comput. Math. 5 (2002) 95–126.
[8] G. Hiss, G. Malle, Low-dimensional representations of special unitary groups, J. Algebra 236 (2001) 745–767.
[9] C. Jansen, The minimal degrees of faithful representations of the sporadic simple groups and their covering groups, LMS J. Comput. Math. 8 (2005) 122–144.
[10] C. Jansen, K. Lux, R.A. Parker, R.A. Wilson, An ATLAS of Brauer Characters, Oxford University Press, Oxford, 1995.
[11] P.B. Kleidman, M.W. Liebeck, The Subgroup Structure of the Finite Classical Groups, London Math. Soc. Lecture Note Ser., vol. 129, Cambridge University Press, 1990.
[12] W.M. Kantor, A. Seress, Prime power graphs for groups of Lie type, J. Algebra 247 (2002) 370–434.
[13] M.W. Liebeck, C.E. Praeger, J. Saxl, The maximal factorizations of the finite simple groups and their automorphism groups, Mem. Amer. Math. Soc. 86 (432) (1990).
[14] T. Nagell, Introduction to Number Theory, Wiley and Sons, New York, 1951.
[15] J. Voight, On the nonexistence of odd perfect numbers, in: MASS Selecta, American Mathematical Society, Providence, RI, 2003, pp. 293–300.
[16] Martin Schönert, et al., GAP – Groups, Algorithms, and Programming – version 3 release 4 patchlevel 4, Lehrstuhl D für Mathematik, Rheinisch Westfälische Technische Hochschule, Aachen, Germany, 1997.