J. Group Theory 12 (2009), 119–137
DOI 10.1515/JGT.2008.065

Journal of Group Theory

Intervals in the subgroup lattices of the alternating and symmetric groups of prime degree

Philipp Perepelitsky

(Communicated by R. M. Guralnick)

Abstract. If G is a group and H is a subgroup of G, we write $\mathcal{C}_G(H)$ for the lattice of overgroups of H in G. It is an open question whether or not every finite lattice is isomorphic to some finite group interval lattice $\mathcal{C}_G(H)$, where G is finite. We prove that no $D\Delta(m_1, \ldots, m_t)$-lattice and few M-lattices have the form $\mathcal{C}_G(H)$, where G is an alternating or symmetric group of prime degree.

1 Introduction

If G is a group and H is a subgroup of G, we write $\mathcal{C}_G(H)$ for the lattice of overgroups of H in G. If G is finite, such a lattice is called a *finite group interval lattice*. The following question has received a lot of attention during the last 25 years:

Question. Is every finite lattice isomorphic to a finite group interval lattice?

The following theorem proved by Palfy and Pudlak in [13] provides motivation from the study of congruence lattices of finite algebras.

Theorem. *The following are equivalent*:

(1) *the Question has a positive answer*;

(2) *every finite lattice is isomorphic to the congruence lattice of a finite algebra.*

For a discussion of congruence lattices of algebras, see [8].

There are results in the literature which reduce the Question for two classes of lattices to the class of almost simple groups, together with some related questions for almost simple groups. We next describe these two classes of lattices.

For $n \in \mathbb{N}$, let M_n denote the lattice of size $n + 2$ in which every element that is not the greatest or the smallest is maximal. Call such a lattice an *M-lattice*.

Now it is known that the set S of natural numbers n for which M_n is isomorphic to a finite group interval lattice is infinite, but it is conjectured that S is relatively small.

If this conjecture is true, then the class of M-lattices would provide a class of counter-examples to the Question. In [3], a reduction is given to the almost simple case for M-lattices, plus some related questions for almost simple groups.

Let Λ be a finite lattice. Then Λ has a least element 0 and a greatest element ∞. We denote the set $\Lambda - \{0, \infty\}$ by Λ'. We say that Λ is *connected* if the graph $(\Lambda', \leqslant \text{or} \geqslant)$ is connected.

Let $\Delta(n)$ denote the lattice of subsets of an n-set. We say that a lattice Λ is a $D\Delta(m_1, \ldots, m_t)$-*lattice* for $t > 1$ and $m_i > 2$ if Λ has t connected components, $\Lambda_1, \ldots, \Lambda_t$, and $\Lambda_i \cong \Delta(m_i)'$ for all i.

In [2], the Question for the class of $D\Delta(m_1, \ldots, m_t)$-lattices is reduced to the case of almost simple groups, plus the non-existence of the so-called 'signalizer lattices' in almost simple groups, isomorphic to $D\Delta(m_1, \ldots, m_t)$-lattices.

The alternating and symmetric groups are almost simple, and are the obvious first test case for analyzing the Question.

Let Λ be a finite lattice of size greater than 2. Then we say that Λ is an *I-lattice* if for every maximal element $x \in \Lambda'$, there is a maximal element $y \in \Lambda'$ such that $x \wedge y = 0$.

Note that disconnected lattices are I-lattices, so in particular M-lattices and $D\Delta(m_1, \ldots, m_t)$-lattices are I-lattices. Therefore, the class of I-lattices represents a convenient domain in which one can simultaneously analyze M-lattices and $D\Delta(m_1, \ldots, m_t)$-lattices.

The *depth* of a subgroup H of a finite group G is the length of the longest chain in $\mathcal{C}_G(H)$.

The following theorem and corollary were proved by Aschbacher in [2].

Theorem. *Let $\mathcal{I}$ be the set of I-lattices Λ such that $\Lambda \cong \mathcal{C}_G(H)$ for some alternating or symmetric group G of finite non-prime degree, and some primitive subgroup H of G. Then $\mathcal{I}$ is small and can be enumerated. In particular, $\mathcal{I}$ contains no $D\Delta(m_1, \ldots, m_t)$-lattice and only one M-lattice.*

Corollary. *Let G be an alternating or symmetric group of finite non-prime degree, and H a primitive subgroup of G of depth 2. Then H is contained in at most two maximal subgroups of G.*

Thus to complete the picture, one must analyze lattices of the form $\mathcal{C}_G(H)$, where G is a symmetric or alternating group of prime degree. This is done in this paper; the main results are the following (see Theorems 6.8, 6.9, Lemma 7.12 and Theorem 7.14):

Theorem 1. *The set of I-lattices that are isomorphic to $\mathcal{C}_S(H)$, where S is a symmetric group of prime degree and $H \leqslant S$, is small and can be enumerated.*

Theorem 2. *Let Ω be a finite set of prime order. Let $G = \mathrm{Sym}(\Omega)$ or $\mathrm{Alt}(\Omega)$. Then for $H \leqslant G$, $\mathcal{C}_G(H)$ is not a $D\Delta(m_1, \ldots, m_t)$-lattice.*

Theorem 3. *For $n \in \mathbb{N}$, the following are equivalent:*

(1) *there exists a set Ω of prime order, a group $G \in \{\mathrm{Sym}(\Omega), \mathrm{Alt}(\Omega)\}$, and a subgroup $H \leqslant G$ such that $\mathcal{C}_G(H) \cong M_n$;*

(2) $n \in \{1, 2, 3, 4, 5, 7, 11\}$.

Corollary 4. *Let G be an alternating or symmetric group of prime degree, and M a subgroup of G of depth 2. Then M is contained in exactly 1, 2, 3, 4, 5, 7 or 11 maximal subgroups of G.*

Let Ω be a finite set, let $l = |\Omega|$, and let $S = \mathrm{Sym}(\Omega)$ and $A = \mathrm{Alt}(\Omega)$. This notation will be in force throughout the paper.

2 Lattice-theoretic preliminaries

Given two finite lattices Λ_1 and Λ_2, write $\Lambda_1 * \Lambda_2$ for the lattice Λ such that the poset Λ' is the disjoint union of the posets Λ_1' and Λ_2'. Let $\hat{\Lambda}_1$ denote the lattice obtained by adjoining a greatest element above Λ_1. For $n \in \mathbb{N}$, write T_n for the tower of size $n+2$, and write $\Xi(n)$ for the overgroup lattice of the subgroup generated by an n-cycle in S_n.

3 Partitions and the symmetric group

Let $G \in \{A, S\}$. Let $\mathscr{S}$ be the lattice of all subgroups of S. For $H \leqslant S$ acting on $X \subseteq \Omega$, let H^X be the subgroup of $\mathrm{Sym}(X)$ induced by H.

Let $\mathscr{P}$ be the lattice of partitions of Ω, where for $P, Q \in \mathscr{P}$, we write $P \leqslant Q$ if and only if each block of P is a union of blocks of Q. For $\Sigma \in \mathscr{P}$, let

$$N_G(\Sigma) = \{g \in G : g\Sigma = \Sigma\}$$

and

$$C_G(\Sigma) = \{g \in G : gD = D \text{ for all blocks } D \text{ of } \Sigma\}.$$

Define the *type* of Σ to be the sequence $a_1^{k_1}, \ldots, a_n^{k_n}$, where $a_1 > \cdots > a_n$ and Σ has exactly k_i blocks of size a_i.

For non-empty proper subsets B and C of Ω, let $N_G(B) = \{g \in G : gB = B\}$, $C_G(B) = \{g \in G : gb = b \text{ for all } b \in B\}$, $\bar{B} = \Omega - B$, $P_B = \{B, \bar{B}\}$, and $P_{B,C} = P_B \vee P_C$.

Lemma 3.1. *Let L be a primitive subgroup of S. If L contains a transposition, then $L = S$, and if L contains a 3-cycle, then $A \leqslant L$.*

Proof. See [6, Theorem 3.3A]. □

Theorem 3.2. (1) *A subgroup M of G is maximal in G if and only if exactly one of the following holds:*

(a) *$M = N_G(B)$ for some non-empty $B \subset \Omega$ such that $|B| \neq l/2$;*

(b) *$M = N_G(\Sigma)$ for some regular $\Sigma \in \mathscr{P}'$ such that $G = S$ or Σ is not of type 2^4;*

(c) *M is a maximal primitive subgroup of G;*

(2) *For all $B \subset \Omega$ such that $|B| = l/2$, $\mathscr{O}_G(N_G(B))' = \{N_G(P_B)\}$.*

Proof. If M is a maximal subgroup of G, then it follows from the definition of primitivity that M is of type (a), (b) or (c). Conversely, if $M \leqslant G$ is of type (a), (b) or (c), then the maximality of M in G essentially follows from Lemma 3.1. Thus (1) holds. Similarly, (2) follows easily from (1) and Lemma 3.1. □

Lemma 3.3. *If $L \leqslant S$ is primitive and non-abelian, and L has one quasi-equivalence class of faithful transitive representations of degree l (i.e.* Aut(L) *is transitive on subgroups H of index l) then*

(1) *S is transitive on its transitive subgroups isomorphic to L, and*

(2) *$N_S(L)$ is isomorphic to the normalizer in* Aut(L) *of H^L via the conjugation representation of $N_S(L)$ on L.*

Proof. Note that (1) follows from the definition of quasi-equivalence and (2) follows from [6, Theorems 4.2A and 4.2B]. □

Suppose that $\Omega = \mathbb{F}_q^d$. Then for $a \in \mathrm{GL}_d(q)$ and $v \in \Omega$, define $t_{a,v} : \Omega \to \Omega$ by $\beta \mapsto a\beta + v$. Let $\mathrm{AGL}_d(q) = \{t_{a,v} : a \in \mathrm{GL}_d(q), v \in \Omega\}$. One may easily show that $\mathrm{AGL}_d(q)$ is a 2-transitive subgroup of S, called the *affine group of degree d over $\mathbb{F}_q$*.

4 Intersections of set stabilizers

We retain the notation of Section 3. In particular, $G \in \{A, S\}$. Assume that $l > 4$. Let $\varnothing \neq B$, $C \subset \Omega$ and suppose that $B \notin \{C, \bar{C}\}$. Let $H = H_G = N_G(B) \cap N_G(C)$. Let $P = P_{B,C}$. Define $C_G : \mathscr{P} \to \mathscr{S}$ by $Q \mapsto C_G(Q)$.

Lemma 4.1. $H = C_G(P)$.

Proof. The result comes from [11, Lemma 3.1], but the proof is easy. □

Lemma 4.2. (1) *If $P_1, P_2 \in \mathscr{P}$ satisfy $P_1 \leqslant P_2$, then $C_G(P_2) \leqslant C_G(P_1)$.*

(2) *Let $\mathscr{Q}_S = \mathscr{P}$ and let $\mathscr{Q}_A = \{Q \in \mathscr{P} : Q$ is not of type $2, 1^{l-2}\}$. Then C_G is injective on $\mathscr{Q}_G$ and a dual map of posets.*

Proof. (1) Each block of P_1 is a union of blocks of P_2, and so $C_G(P_2) \leqslant C_G(P_1)$.

(2) For $Q \in \mathscr{Q}_G$, the orbits of $C_G(Q)$ on Ω are the blocks of Q, so C_G is injective on $\mathscr{Q}_G$. □

Theorem 4.3. (1) *If* $|P| = 4$, *then*

(a) $\mathcal{C}_G(H)$ *is connected, and*

(b) *if* l *is prime and* $G = S$, *then* $\mathcal{C}_S(H)$ *is not an* l*-lattice.*

(2) *If* $\mathcal{C}_G(H) \cong M_n$, *then* $n = 3$.

(3) $\mathcal{C}_G(H)$ *is not a* $D\Delta(m_1, \ldots, m_t)$*-lattice.*

(4) *If* l *is prime and* $|P| = 3$ *then either*

(a) $G = A$, $l = 5$, $|H| = 2$, $\mathcal{C}_A(H) \cong M_4 * T_2$ *or*

(b) *each proper overgroup of* H *is intransitive and* $\mathcal{C}_G(H) \cong M_3$ *or* $M_2 * T_2$.

Proof. First note that $|P| = 3$ or 4. As $H = C_G(P)$ by Lemma 4.1, it follows that

(*) if M is a maximal transitive but imprimitive member of $\mathcal{C}_G(H)$, then for some block D of P, $H < N_M(D)$.

(1) Let $Y = \{Q \in \mathcal{P} : Q \leqslant P\}$. If P is of type 2, 1^3 and $G = A$, then $H = 1$, and one can check that (1) holds. Therefore we may assume that this is not the case, so that $Y \subseteq \mathcal{Q}_G$, and hence H acts transitively on each member of P and $C_G : Y \to \mathcal{C}_G(H)$ is an injective dual map of posets by Lemma 4.2. It follows that

(**) each maximal intransitive member of $\mathcal{C}_G(H)$ is contained in $C_G(Y)'$ and as Y is clearly connected, the poset of intransitive members of $\mathcal{C}_G(H)'$ is connected.

Therefore by (*),

(***) the subposet consisting of the imprimitive members of $\mathcal{C}_G(H)'$ is connected.

Now if P does not have a block of size greater than 2, then using (***) and a knowledge of the primitive permutation groups of degree at most 8, one may verify directly that (a) holds. Hence we may assume that P has a block of size at least 3, so by Lemma 3.1, H has a 3-cycle and hence $\mathcal{C}_G(H)'$ has no primitive members. Therefore, by (***), (a) holds, so it remains to prove (b).

Suppose that l is prime and that $G = S$. Then $H = C_S(P)$ contains a transposition, so by Lemma 3.1, each member of $\mathcal{C}_S(H)'$ is intransitive. Therefore by (**), for each block D of P, there is no maximal member M of $\mathcal{C}_S(H)$ such that $N_M(D) = H$, so (b) holds.

(2), (3) and (4) If $|P| = 4$, then (2), (3) and (4) hold by (1). Therefore, we may assume that $|P| = 3$. Let $P = \{X_1, X_2, X_3\}$. Now H acts transitively on each member of P, and hence

(i) the maximal intransitive members of $\mathcal{C}_G(H)$ are the subgroups $N_G(X_i)$, and by Lemma 4.1, for i, j distinct we have $H = N_G(X_i) \cap N_G(X_j)$.

Let $1 \leqslant i \leqslant 3$ and let $\{j, k\} = \{1, 2, 3\} - \{i\}$. We claim that

(ii) one of the following holds:

(I) $|X_j| = |X_k|$ and $\mathcal{C}_{N_G(X_i)}(H) \cong T_1$;

(II) $|X_j| \neq |X_k|$ and H is maximal in $N_G(X_i)$.

To prove this we note that $C_G(X_j \cup X_k)$ is the kernel of the action of $N_G(X_i)$ on $X_j \cup X_k$ and $C_G(X_j \cup X_k) \leqslant H$, so $\mathcal{O}_{N_G(X_i)}(H) \cong \mathcal{O}_{N_G(X_i)^{X_j \cup X_k}}(H^{X_j \cup X_k})$, and the claim holds by Theorem 3.2.

(3) Let $1 \leqslant i \leqslant 3$ and suppose that $|X_i| \neq l/2$. Then by Theorem 3.2, $N_G(X_i)$ is maximal in G. Now by (ii), $\mathcal{O}_{N_G(X_i)}(H) \cong T_0$ or T_1, and (3) holds in each case.

(4) If P is of type 2^2, 1 and $G = A$, then $|H| = 2$ and using (ii), it is not hard to show that (a) holds. Therefore, we assume that this is not the case, so that H contains a 3-cycle and hence by Lemma 3.1, every member of $\mathcal{O}_G(H)'$ is intransitive. Then as l is prime, P must have a pair of members with distinct orders, so by (i) and (ii), (b) holds.

(2) Suppose that $\mathcal{O}_G(H) \cong M_n$. Then by (*), $\mathcal{O}_G(H)$ does not have any transitive but imprimitive members. If P does not have a block of size greater than 2, then using (4) and a knowledge of the subgroups of A_6, one may show that $\mathcal{O}_G(H)$ is not an M-lattice, a contradiction. Therefore, P has a block of size greater than 2, so that H contains a 3-cycle and hence $\mathcal{O}_G(H)'$ has no primitive members. Therefore, each member of $\mathcal{O}_G(H)'$ is intransitive, so (2) holds by (i). □

5 Transitive actions of prime degree

Lemma 5.1. *Assume that $l = p$ is prime and let G be a non-abelian simple subgroup of S. Then G is isomorphic to exactly one of the following groups and S is transitive on its transitive subgroups isomorphic to G:*

(a) A;

(b) $\mathrm{PSL}_d(q)$ *where $d \in \mathbb{N}$ and q is a prime power such that $(q^d - 1)/(q - 1) = p$;*

(c) $\mathrm{PSL}_2(11)$;

(d) M_{23};

(e) M_{11}.

Proof. See [9, Theorem 1 and the following remark]. Note that the fact that G has one quasi-equivalence class of representations of degree p implies the transitivity by Lemma 3.3. □

In view of case (b) in Lemma 5.1, it is of interest to know when $(q^d - 1)/(q - 1)$ is a prime, where $d \in \mathbb{N}$ and q is a prime power.

Lemma 5.2. *Let r be a prime and b be a positive integer. One of the following holds:*

(a) *there is a prime $s \mid r^b - 1$ with $s \nmid r^c - 1$ for $c < b$;*

(b) *$r = 2$ and $b = 6$;*

(c) *r is a Mersenne prime and $b = 2$.*

Proof. See [14]. □

Lemma 5.3. *Let $q = r^m$ be a prime power and $d \in \mathbb{N}$. If $(q^d - 1)/(q - 1)$ is prime, then d is prime, $d \nmid q - 1$, and m is a power of d.*

Proof. For $a \in \mathbb{N}$ such that $a|d$ we have $(q^a - 1)/(q - 1) \mid (q^d - 1)/(q - 1)$, and hence d is prime. If $d \mid q - 1$, then $q \equiv 1 \pmod{d}$ and hence d divides $\sum_{0 \leqslant i \leqslant d-1} q^i = (q^d - 1)/(q - 1)$, a contradiction. Therefore, $d \nmid q - 1$, and it remains to show that m is a power of d.

Assume the contrary, and let $m = d^i a$, where $i \geqslant 0$, $a > 1$ and $(a, d) = 1$. By Lemma 5.2, we may assume that there is a prime s such that r has order d^{i+1} in $(\mathbb{Z}/s\mathbb{Z})^\times$. In particular, as $q = r^{d^i a}$, we have $s \mid q^d - 1$ and $s \nmid q - 1$. Therefore, as $(q^d - 1)/(q - 1)$ is prime, $(q^d - 1)/(q - 1) = s \mid r^{d^{i+1}} - 1$, and so

$$r^{d^{i+1}a} - 1 \leqslant (r^{d^{i+1}} - 1)(r^{d^i a} - 1) = r^{d^i(a+d)} - r^{d^{i+1}} - r^{d^i a} + 1.$$

This contradicts the fact that $ad > a + d$ as $a > 1$. Therefore, m is a power of d. □

Lemma 5.4. *Let q be a prime power and let $d \in \mathbb{N}$. Then*

(1) $(q^d - 1)/(q - 1) \neq 11, 23$;

(2) $(q^d - 1)/(q - 1) = 13$ *if and only if* $(q, d) = (3, 3)$;

(3) $(q^d - 1)/(q - 1) = 31$ *if and only if* $(q, d) = (2, 5)$ *or* $(5, 3)$.

Proof. This is straightforward. □

Lemma 5.5. *Assume that l is prime. Let $H < G \leqslant S$ be almost simple with $A \not\leqslant G$. Then* $\mathrm{soc}(G) = \mathrm{soc}(H)$ *unless* $p = 11$, $H \cong \mathrm{PSL}_2(11)$ *and* $G \cong M_{11}$.

Proof. See [12] in conjunction with Lemma 5.1. □

Lemma 5.6. *Let V be a finite-dimensional vector space over a finite field. Assume that Ω is the set of points of* $\mathrm{PG}(V)$. *Let $L = \mathrm{PSL}(V)$ and let $\Gamma = \mathrm{P\Gamma L}(V)$. Then*

(1) $N_S(L) = \Gamma$, *and*

(2) $N_S(\Gamma) = \Gamma$.

Proof. (1) Let σ be the transpose-inverse automorphism of L. Then by [7, Theorem 2.5.12], $\mathrm{Aut}(L) = G\langle\sigma\rangle$, where G is the image of the action of Γ on L by conjugation. Hence by Lemma 3.3 we have $G \leqslant N$, where N is the normalizer in $\mathrm{Aut}(L)$ of H^L, where H is a point stabilizer in L. Now if $d = 2$, then $\sigma \in G$ and $\Gamma \cong G = N \cong N_S(L)$ by Lemma 3.3, and if $d > 2$, then σ maps the stabilizer of a point in L to the stabilizer of a hyperplane in L, and hence $\sigma \notin N$. Therefore, $N = G \cong \Gamma$, so by Lemma 3.3, $\Gamma = N_S(L)$.

Now note that (2) follows from (1) and the fact that L is characteristic in Γ. □

For the remainder of the section, assume that $l = p$ is prime.

Lemma 5.7. *If $G < A$ is non-abelian and simple, then $N_S(G) < A$ and if $G \cong M_{23}$ or M_{11} or $\mathrm{PSL}_2(11)$, then $N_S(G) = G$.*

Proof. The group G is listed in one of the cases (b)–(e) of Lemma 5.1. By [5], if $G \cong M_{23}$ or M_{11}, then $G \cong \mathrm{Aut}(G)$, so $G = N_S(G)$ by Lemma 3.3. This completes the treatment of cases (d) and (e).

Assume that $G \cong \mathrm{PSL}_2(11)$. Then there are two classes of subgroups of G of index 11, which are fused in $\mathrm{Aut}(G)$, so $[\mathrm{Aut}(G) : N_S(G)] = 2$ by Lemma 3.3. By [5], $[\mathrm{Aut}(G) : G] = 2$, so $G = N_S(G)$, completing the treatment of (c). Hence we may assume that G is of type (b) of Lemma 5.1.

By Lemma 5.6, $N_S(G) \cong \mathrm{P\Gamma L}_d(q)$, so $|N_S(G)/G| = m$ by Lemma 5.3. If d is odd, then m is odd by Lemma 5.3, so $N_S(G) < A$ as $G < A$. Therefore, as d is prime, we may assume that $d = 2$. As $q + 1$ is prime, $q = 2^{2^a}$ for some $a \in \mathbb{N}$. Hence $\mathrm{P\Gamma L}_2(q) = \mathrm{PSL}_2(q)\Phi$, where Φ denotes the group of automorphisms of $\mathrm{PG}_1(q)$ induced by $\mathrm{Aut}(\mathbb{F}_q)$. Therefore, it suffices to show that the generator σ of Φ acts as an even permutation on the points of $\mathrm{PG}_1(q)$.

View $\mathbb{F}_q^2$ as the vector space of ordered pairs of members of $\mathbb{F}_q$. Then each point $\langle(1, \beta)\rangle$ of $\mathrm{PG}_1(q)$ belongs to a cycle of σ of length 2^r, where $r \leqslant a$ is minimal subject to $\beta \in \mathbb{F}_{2^{2^r}}$. Therefore, for $2 \leqslant 2^r \leqslant 2^a$, there are exactly $(|\mathbb{F}_{2^{2^r}}^\times| - |\mathbb{F}_{2^{2^{r-1}}}^\times|)/2^r = 2^{2^r - r} - 2^{2^{r-1} - r}$ cycles of length 2^r in the cycle decomposition of σ. Hence as $a \geqslant 2$, σ has an even number of cycles of even length, and hence is an even permutation. □

Lemma 5.8. *Suppose that $G < S$ is affine and let $H = G \cap A$. Then*

(1) *G is maximal in S, and*

(2) *exactly one of the following holds:*
   (a) *$p \neq 7, 11, 17, 23$ and H is maximal in A;*
   (b) *$p = 7$ or 17, and $\mathcal{O}_A(H)' \subseteq \Gamma^S$, where Γ is a projective semilinear subgroup of A;*
   (c) *$p = 23$, and $\mathcal{O}_A(H)' \subseteq M^S$ for some $M < A$ such that $M \cong M_{23}$;*
   (d) *$p = 11$, and $H \leqslant L \leqslant M$ for some $L, M \leqslant A$ such that $L \cong \mathrm{PSL}_2(11)$ and $M \cong M_{11}$; furthermore, $\mathcal{O}_A(H)' \subseteq L^S \cup M^S$.*

Proof. This follows from [12, Table I], and the transitivity statements in Lemma 5.1. □

Lemma 5.9. *For all transitive subgroups G of S, exactly one of the following holds:*

(1) *G is a subgroup of an affine subgroup of S;*

(2) *G is almost simple, and exactly one of the following holds:*
   (a) *$G = A$ or S;*
   (b) *$G \cong M_{11}, M_{23}$ or $\mathrm{PSL}_2(11)$;*
   (c) *$\mathrm{PSL}_d(q) \leqslant G \leqslant \mathrm{P\Gamma L}_d(q)$ for some $d \in \mathbb{N}$ and some prime power q such that $(q^d - 1)/(q - 1) = p$.*

Proof. This follows from two results of Burnside (see [6, Theorem 3.5B, Corollary 3.5B, Theorems 4.1A, 4.1B]), along with Lemmas 5.1, 5.6 and 5.7. □

As l is prime, each transitive subgroup of S is primitive on Ω. Hence the following lemmas follow from Lemmas 5.9, 5.8, 5.5, 5.7 and Theorem 3.2.

Lemma 5.10. *A subgroup G of S is maximal in S if and only if one of the following holds:*

(1) $G = A$;

(2) *G is affine;*

(3) $G = N_S(B)$ *for some set B with* $\varnothing \neq B \subset \Omega$.

Lemma 5.11. *A subgroup G of A is maximal in A if and only if one of the following holds:*

(1) $G \cong M_{11}, M_{23}$, *or G is projective semilinear;*

(2) $G = A \cap K$, *where K is affine and* $p \neq 7, 11, 17, 23$;

(3) $G = N_A(B)$ *for some* $\varnothing \neq B \subset \Omega$.

6 The overgroup lattice $\mathscr{O}_S(H)$

The notation with Ω, l, S and A and the assumption that $l = p > 3$ is prime are in force throughout this section and the remainder of the paper.

Lemma 6.1. *Let G be an affine subgroup of S. Then every intransitive subgroup of G is cyclic and stabilizes a point.*

Proof. Let $X \leqslant G$ be intransitive, and let K be the subgroup of G of order p. Then as $X \cap K = 1$ we have

$$X \cong X/(X \cap K) \cong XK/K \leqslant G/K \cong Z_{p-1},$$

so X is cyclic. Also as K is the Frobenius kernel of the Frobenius group G and $X \not\leqslant K$, X stabilizes a point. □

Lemma 6.2. *If $H \leqslant K \leqslant S$ and K is transitive on $H^S \cap K$, then $N_S(H)$ is transitive on $\Delta = \{L \in \mathscr{O}_S(H) : L \in K^S\}$, and $|\Delta| = [N_S(H) : N_S(H) \cap N_S(K)]$.*

Proof. Let $L \in \Delta$ and choose $x \in S$ such that $K^x = L$, and $k \in K$ such that $H^k = H^{x^{-1}}$. Then $K^{xk} = (K^k)^x = L$ and $H^{xk} = (H^k)^x = H$, so $xk \in N_S(H)$ and hence $N_S(H)$ is transitive on Δ. Therefore, by the orbit–stabilizer lemma, $|\Delta| = [N_S(H) : N_S(H) \cap N_S(K)]$. □

Lemma 6.3. *Let $G \leqslant S$ be affine and let $\omega \in \Omega$. Then there are exactly $\phi(p-1) = [N_S(G_\omega) : G_\omega]$ affine subgroups of S that contain G_ω, where ϕ is the Euler phi-function.*

Proof. By 6.2, the number of affine subgroups of S that contain G_ω is $[N_S(G_\omega) : G_\omega]$. Let $G_\omega = \langle y \rangle$. As y is a $(p-1)$-cycle, $N_S(G_\omega)$ acts transitively on the $\phi(p-1)$ conjugates of $y \in G_\omega$, so $[N_S(G_\omega) : C_S(y)] = \phi(p-1)$. Now as the number of $(p-1)$-cycles in S is $p!/(p-1)$, we have $|C_S(y)| = |S|(p-1)/p! = p-1$. Therefore, $|N_S(G_\omega)| = \phi(p-1)(p-1)$, so $[N_S(G_\omega) : G_\omega] = \phi(p-1)$. □

Lemma 6.4. *If H is a transitive subgroup of an affine subgroup G of S, then $G = N_S(H)$.*

Proof. Let K be the subgroup of G of order p. As H is transitive, $K \leqslant H$. If $\omega \in \Omega$ then $G = G_\omega K$, so $H = H_\omega K$. As G_ω is cyclic, $H_\omega \trianglelefteq G_\omega$, so $H = H_\omega K \trianglelefteq G_\omega K = G$. Therefore $G = N_S(H)$ by the maximality of G, completing the proof. □

Lemma 6.5. *Let G be an affine subgroup of S and let $H = G \cap A$. Then exactly one of the following holds:*

(1) $p \notin \{7, 11, 17, 23\}$, $\mathcal{O}_A(H) \cong T_0$, *and* $\mathcal{O}_S(H) \cong M_2$;

(2) $p = 7$ *or* 17 *or* 23, $\mathcal{O}_A(H) \cong M_2$, *and* $\mathcal{O}_S(H) \cong \hat{M}_2 * T_1$;

(3) $p = 11$, $\mathcal{O}_A(H) \cong T_2 * T_2$, *and* $\mathcal{O}_S(H) \cong \widehat{T_2 * T_2} * T_1$.

Proof. By Lemma 6.4, G is the unique affine member of $\mathcal{O}_S(H)$, and hence by Lemma 5.10, $\mathcal{M} = \{G, A\}$, where $\mathcal{M}$ is the set of maximal members of $\mathcal{O}_S(H)$. Note that as H is maximal in G, we have

(*) $\mathcal{O}_S(H) \cong \hat{\mathcal{O}}_A(H) * T_1$.

Now we claim the following:

(**) Let $D = N_S(R)$ for some non-abelian simple group $R < A$. If $H \leqslant D$, then $|D^S \cap \mathcal{O}_S(H)| = 2$.

For the proof of the claim let K be the Frobenius kernel of G. Then by Lemma 6.4, $G = N_S(K) = N_S(H)$ and hence $H = N_A(K) = N_D(K)$ by Lemma 5.7. Hence as K is a Sylow subgroup of D, $H^S \cap D = H^D$. Therefore, by Lemma 6.2, $|D^S \cap \mathcal{O}_S(H)| = [G : H| = 2$, and so (**) holds.

If $p \notin \{7, 11, 17, 23\}$ or if $p \in \{7, 17, 23\}$, then it follows from Lemma 5.8, (**) and (*) that (1) and (2) hold respectively, so we may assume that $p = 11$.

By [5], $L^S \cap M = L^M$, so by Lemmas 5.7 and 6.2 we have $|M^S \cap \mathcal{O}_S(L)| = 1$. Therefore, by (*), (**) and Lemma 5.8, (3) holds, and the proof is complete. □

Lemma 6.6. *If $H = N_A(B)$ for some non-empty $B \subset \Omega$, then $\mathcal{O}_S(H) \cong M_2$.*

Proof. Recall that $p > 3$, so $N_S(B)$ is the unique maximal intransitive member of $\mathcal{O}_S(H)$, and H contains a 3-cycle, so A is the unique transitive member of $\mathcal{O}_S(H)'$ by Lemma 3.1. The lemma now holds by Lemma 5.10. □

Lemma 6.7. *Let $G \leqslant S$ be affine and let $H = G_\omega$ for some $\omega \in \Omega$. Then*

$$\mathscr{C}_S(H) \cong M_{\phi(p-1)} * \Xi(\widehat{p-1}),$$

where ϕ is the Euler phi-function.

Proof. By Lemma 5.10 we have $\mathscr{M} = \{S_\omega\} \cup (G^S \cap \mathscr{C}_S(H))$, where $\mathscr{M}$ is the set of maximal members of $\mathscr{C}_S(H)$. The lemma now follows from Lemma 6.3. □

Theorem 6.8. *For $H \leqslant S$, $\mathscr{C}_S(H)$ is an I-lattice if and only if exactly one of the following holds*:

(1)(a) $\mathscr{C}_S(H) \cong M_2$;

(b) $\mathscr{C}_S(H) \cong \hat{M}_2 * T_1$;

(c) $\mathscr{C}_S(H) \cong \widehat{T_2 * T_2} * T_1$;

(2) $\mathscr{C}_S(H) \cong M_3$ *or* $M_2 * T_2$;

(3) $\mathscr{C}_S(H) \cong M_{\phi(p-1)} * \Xi(\widehat{p-1})$, *where ϕ is the Euler phi-function.*

Proof. Let $H \leqslant S$ such that $\mathscr{C}_S(H)$ is an I-lattice and let $\mathscr{M}$ be the set of maximal members of $\mathscr{C}_S(H)$. Then as $\mathscr{C}_S(H)$ is an I-lattice, by Lemma 5.10, one of the following holds:

(I) $H = G \cap A$ for some affine $G \leqslant S$;

(II) $H = N_A(B)$ for some set B with $\varnothing \neq B \subset \Omega$;

(III) $H = N_S(B) \cap N_S(C)$ for some non-empty sets $B, C \subset \Omega$ such that $B \notin \{C, \bar{C}\}$;

(IV) $H = G \cap M$ for some affine $G \leqslant S$ and some $M \in \{N_S(B) : \varnothing \neq B \subset \Omega\} \cup G^S$.

In case (I), (1) holds by Lemma 6.5, and in case (II), (1)(a) holds by Lemma 6.6. In case (III), (2) holds by Theorem 4.3, so we may assume that (IV) holds. Then by Lemmas 6.1 and 6.4, we have $H = S_\omega \cap M_2$ for some $M_2 \in \mathscr{M}$ and some $\omega \in \Omega$. Therefore by Lemma 5.10 and our analysis of case (III), we may assume that $H = L_\omega$ for some affine $L \leqslant S$. Therefore (3) holds, by Lemma 6.7. □

Theorem 6.9. *For $n \in \mathbb{N}$, the following are equivalent*:

(1) *there exists a set Ω of prime order and a subgroup H of $S = \mathrm{Sym}(\Omega)$ such that $\mathscr{C}_S(H) \cong M_n$;*

(2) $1 \leqslant n \leqslant 4$.

Proof. This follows from Theorem 6.8 and the fact that the lattice of subgroups of S_3 is isomorphic to M_4. □

7 The overgroup lattice $\mathscr{C}_A(H)$

The notation with Ω, $l = p > 3$, A and S is in force throughout this section.

Lemma 7.1. *Let M be a transitive subgroup of A and let $H = N_M(B)$, where B is a proper non-empty subset of Ω such that $|B| \geqslant 3$. If $H^{\bar{B}} \neq \mathrm{Sym}(\bar{B})$, then H is not maximal in $N_A(B)$.*

Proof. As M is transitive, M and hence H does not contain a 3-cycle by Lemma 3.1. Therefore, $H < \{x \in N_A(B) : x^{\bar{B}} \in H^{\bar{B}}\} < N_A(B)$, and hence H is not maximal in $N_A(B)$. □

Lemma 7.2. *Suppose that $p = 11$ and let $H \leqslant A$.*

(1) *If $H = M_\alpha$ for some $M \leqslant A$ such that $M \cong M_{11}$ and some $\alpha \in \Omega$, then $\mathcal{C}_A(H) \cong M_3$.*

(2) *If $H \cong \mathrm{PSL}_2(11)$, then $\mathcal{C}_A(H) \cong M_1$.*

Proof. (1) Note that $H \cong M_{10}$ and hence by [4], we have $\mathrm{PSL}_2(9) \cong H' \operatorname{char} H$. By Lemma 5.6, $N_S(H') \cong \mathrm{P\Gamma L}_2(9)$, so $[N_S(H') : H] = 2$ and $N_S(H) = N_S(H')$. Also $\mathrm{soc}(H) = H' \cong \mathrm{PSL}_2(9)$ and as $[N_S(H') : H] = 2$ and $N_S(H') \not\leqslant A$ we have $H = N_A(H')$. Hence by [12], H is maximal in $A_\alpha \cong A_{10}$. Therefore as H is transitive on $\Omega - \{\alpha\}$, A_α is the unique maximal intransitive member of $\mathcal{C}_A(H)$, while by Lemmas 5.4 and 5.11, each maximal transitive overgroup M of H is isomorphic to M_{11}. Therefore, by Lemma 6.2, $\mathcal{C}_A(H) \cong M_n$, where $n = 1 + [N_S(H) : H] = 3$.

(2) By [5], $H \leqslant M \cong M_{11}$ and all copies of $\mathrm{PSL}_2(11)$ contained in M are conjugate under M. The result now follows from Lemmas 5.7, 5.11 and 6.2. □

Lemma 7.3. *If $p = 11$, then for $n \in \mathbb{N}$, there exists a subgroup $H \leqslant A$ such that $\mathcal{C}_A(H) \cong M_n$ if and only if $n = 1$ or 3.*

Proof. By Lemma 7.2, for $n = 1, 3$, there exists a subgroup $H \leqslant A$ such that $\mathcal{C}_A(H) \cong M_n$, so it remains to prove the converse. Suppose that $H \leqslant A$ and $\mathcal{C}_A(H) \cong M_n$ for some $n \in \mathbb{N}$. If H is transitive, then by Lemmas 5.4, 5.9 and 5.11, either $H \cong \mathrm{PSL}_2(11)$ or H is contained in an affine subgroup G. In the first case, $\mathcal{C}_A(H) \cong M_1$ by Lemma 7.2. In the second case, Lemma 5.8(d) shows that $G \cap A < L < M < A$ for suitable subgroups L, M of A, so $\mathcal{C}_A(H)$ is not a lattice M_n. Thus we may assume that $H = N_M(B)$ for some non-empty set $B \subset \Omega$ and some maximal overgroup M of H. By Theorem 4.3, we may assume that M is transitive on Ω, so M is M_{11} by Lemmas 5.4 and 5.11.

By Lemma 7.1, we have $|B| \neq 3$ as $8! \nmid |M|$ and $|B| \neq 4, 5$ as M is sharply 4-transitive, so that M is faithful on B, and hence of order at most 5!. Therefore, we may assume that $|B| \leqslant 2$. If $|B| = 2$, then H is isomorphic to a subgroup of index 3 in $\mathrm{AGL}_2(3)$ and hence H is not maximal in $N_A(B) \cong S_9$, a contradiction. Therefore, $|B| = 1$, and the lemma holds by Lemma 7.2. □

Lemma 7.4. *Suppose that $p = 23$ and let $H \leqslant A$.*

(1) *If $\mathcal{C}_A(H) \cong M_n$ for some $n \in \mathbb{N}$, then $n \in \{1, 2, 3\}$.*

(2) *$\mathcal{C}_A(H) \cong M_2$ if and only if $H = G \cap A$ for some affine $G \leqslant S$.*

Proof. By Lemma 6.5, $\mathcal{C}_A(H) \cong M_2$ if $H = G \cap A$ for some affine $G \leqslant S$, so it remains to prove the converse and (1). Suppose that $\mathcal{C}_A(H) \cong M_n$ for some $n \in \mathbb{N}$. By Lemmas 5.4 and 5.11,

(*) each maximal transitive subgroup of A is isomorphic to M_{23}.

Thus if H is not in any copy of M_{23} in A, then $n = 1$ or $H = N_A(B) \cap N_A(C)$ for some non-empty sets $B, C \subset \Omega$ such that $B \notin \{C, \bar{C}\}$, and by Theorem 4.3 we have $n = 3$. Hence we may assume that $H \leqslant M$ for some $M \leqslant A$ such that $M \cong M_{23}$.

If H is transitive, then by Lemmas 5.4, 5.8 and 5.9, we have $H = G \cap A$ for some affine $G \leqslant S$ and then $\mathcal{C}_A(H) \cong M_2$ by Lemma 6.5. Hence we may assume that $H = N_M(B)$ for some non-empty set $B \subset \Omega$ with $|B| \leqslant 23/2$.

As $12! \not| |M|$ we have $|B| \leqslant 2$ by Lemma 7.1. If $|B| = 2$, then H is isomorphic to a subgroup of index 3 in $\mathrm{P\Gamma L}_3(4)$, and hence H is not maximal in $N_A(B) \cong S_{21}$, a contradiction. Therefore $B = \{\alpha\}$ for some $\alpha \in \Omega$, so H is transitive on $\Omega - \{\alpha\}$. Thus by (*), $\mathcal{C}_A(H)' \subseteq \{A_\alpha\} \cup M^S$. As H is maximal in A_α we have $H = N_A(H)$, and so as $N_S(H) \not\leqslant A$ and $[\mathrm{Aut}(H) : H] = 2$ by [1, Lemma 18.8], we conclude from Lemmas 5.7 and 6.2 that $n = 3$. □

Lemma 7.5. *Suppose that $q = r^m$ is a prime power and $d \in \mathbb{N}$, and suppose that $(q^d - 1)/(q - 1) = p$ is prime. Then $(p - 1)/2md$ is prime if and only if $(q, d) = (2, 5)$ or $(5, 3)$ or $(3, 3)$.*

Proof. Suppose that $(p - 1)/2md$ is prime. By Lemma 5.3, d is prime, $d \not| q - 1$, and $m = d^i$ for some $i \geqslant 0$. Next note that

(*) $(p - 1)/2md = q(q^{d-1} - 1)/2d^{i+1}(q - 1)$ is prime.

Now as d is prime, either

(I) $(q, d) = 1$, or

(II) $d | q$.

Suppose that (I) holds and q is odd. Then $d \neq 2$, so that d is an odd prime, and hence $(q^{d-1} - 1)/(q - 1)$ is even; and by (*) and (I), we have

$$(q^{d-1} - 1)/(q - 1)2 = d^{i+1}$$

and q is prime. Therefore, $m = 1$ so that $i = 0$ and

(**) $2d - 1 = \sum_{1 \leqslant i \leqslant d-2} q^i$.

By (**), $2d - 1 \geqslant q(d - 2)$. Therefore as q is odd and prime to $d \neq 2$, it follows that that $d = 3$ and $q = 5$, and the lemma holds.

Now assume that q is even. By (*) and (I), we have $d^{i+1} | (q^{d-1} - 1)/(q - 1)$ and $q(q^{d-1} - 1)/2(q - 1)d^{i+1}$ is prime. Hence, either

(I)(A) $q/2 = 1$ and $(q^{d-1} - 1)/(q-1)d^{i+1}$ is prime, so $q = r = 2$ and hence $m = 1$ and $i = 0$, or

(I)(B) $(q^{d-1} - 1)/(q-1)d^{i+1} = 1$ and $q/2$ is prime so $q = 4$.

If (I)(B) holds, then $d = 2$ as $m = 2$, and so $(d,q) \neq 1$, a contradiction. Therefore (I)(A) holds, and $(2^{d-1} - 1)/d$ is prime, so as $(d,q) = 1$, d is odd and $2^{d-1} - 1 = (2^{(d-1)/2} + 1)(2^{(d-1)/2} - 1)$ is a product of primes. Therefore $(d-1)/2 = 2$ and $d = 5$, so that the lemma holds and hence we may assume that (II) holds.

As $(q^{d-1} - 1)/(q-1) \neq 2$, by (*), $d^{i+1} = q$ and $(q^{d-1} - 1)/2(q-1)$ is prime. Therefore, $i + 1 = d^i$ so that $i = 0$ and hence $d = q$ and $(d^{d-1} - 1)/2(d-1)$ is prime. Thus d is odd, so that $(d^{d-1} - 1)/(d-1) \equiv 0 \pmod 4$. Hence

$$(d^{d-1} - 1)/(d-1) = 4,$$

so that $d = 3$ and the lemma holds. □

Lemma 7.6. *Let $d \in \mathbb{N}$ and $q = r^m$ be a prime power with $(q^d - 1)/(q-1) = p$. Let Γ be a subgroup of A such that $\Gamma \cong \mathrm{P\Gamma L}_d(q)$, let $K \in \mathrm{Syl}_p(\Gamma)$ and let $H = N_\Gamma(K)$. Then*

(1) $|H| = pmd$.

(2) *If $p = 13$ or 31, then $\mathcal{C}_A(H) \cong M_{(p-1)/d+1} = M_5, M_7$ or M_{11}.*

Proof. Note that by [10, (4.33)], H is the projective image of a subgroup of $\mathrm{GL}_d(q)$ isomorphic to $\Gamma\mathrm{L}_1(q^d)$, and so $|H| = pmd$. Hence it remains to prove (2), so we may assume that $p = 13$ or 31. By Lemma 5.4 we have $(q,d) = (3,3)$ if $p = 13$, and $(q,d) = (2,5)$ or $(5,3)$ if $p = 31$. In particular $m = 1$ and $(p-1)/2d$ is prime by Lemma 7.5.

Let $\mathcal{M}$ be the set of maximal members of $\mathcal{C}_A(H)$. If $H \leqslant \Gamma_2 \leqslant A$ and Γ_2 is isomorphic to $\mathrm{P\Gamma L}_k(s)$ where $s = a^b$ is a prime power, then as $m = 1 = b$, by (1) we have $pd = |H|\,|N_{\Gamma_2}(K)| = pk$, so $d = k$ and $q = s$. Therefore by Lemmas 5.11 and 6.4, $\mathcal{M} = \{N_A(K)\} \cup (\Gamma^S \cap \mathcal{C}_A(H))$. Now by [10, (7.3.4)], H is maximal in Γ, and $[N_A(K) : H] = (p-1)/2d$, and so $[N_A(K) : H]$ is prime by an earlier remark. Thus H is maximal in $N_A(K)$. Therefore, $\mathcal{C}_A(H) \cong M_{|\mathcal{M}|}$, and it remains to show that $|\Gamma^S \cap \mathcal{C}_A(H)| = (p-1)/d$. But as $H = N_\Gamma(K)$ and K is a Sylow subgroup of Γ, we have $(H^S \cap \Gamma) = H^\Gamma$, so by Lemma 6.2 we have

$$|\Gamma^S \cap \mathcal{C}_A(H)| = [N_S(K) : N_\Gamma(K)] = (p-1)/d,$$

and (2) holds. □

Lemma 7.7. *Suppose that $p \neq 7, 17$, and that $H \leqslant A$ is transitive and $H \leqslant G \cap \Gamma$ for some affine subgroup G of S and some projective semilinear subgroup $\Gamma \leqslant A$. If $\mathcal{C}_A(H) \cong M_n$ then $n \in \{5, 7, 11\}$.*

Proof. By Lemma 6.4 we have $H = N_\Gamma(K)$, where K is the Frobenius kernel of G. By Lemma 5.4, $p \neq 11$ or 23. Then as $p \neq 7, 17$, the subgroup $G \cap A$ is maximal in A by Lemma 5.11. Thus as $\mathcal{C}_A(H) \cong M_n$, H is maximal in $G \cap A$. Therefore as $(G \cap A)/K$ is cyclic, $[G \cap A : H]$ is prime. Now $|H| = pmd$ by Lemma 7.6, so that $[G \cap A : H] = (p-1)/2md$, and hence $(p-1)/2md$ is prime. Then by Lemmas 5.4 and 7.5 we have $p = 13$ or 31, and so $n \in \{5, 7, 11\}$ by Lemma 7.6. □

Lemma 7.8. *Let V be a 3-dimensional vector space over a finite field of order 2. Let Ω be the set of points of the projective geometry* $\mathrm{PG}(V)$. *Let $\Gamma = \mathrm{P\Gamma L}(V) = \mathrm{PSL}(V)$, let $\Delta \subseteq \Omega$ be a line of* $\mathrm{PG}(V)$, *and let $H = N_\Gamma(\Delta)$. Then $\mathcal{C}_A(H) \cong M_2$.*

Proof. Let $\mathcal{B}$ denote the set of lines of $\mathrm{PG}(V)$. Then the ordered pair $(\Omega, \mathcal{B})$ is the projective plane of order 2 and $\Gamma = \mathrm{Aut}((\Omega, \mathcal{B}))$. It is well known that

(i) $H \cong S_4$ induces $\mathrm{Sym}(\theta)$ on $\theta \in \{\Delta, \bar{\Delta}\}$ and H is transitive on $\mathcal{B} - \{\Delta\}$.

Let $\mathcal{M}$ be the set of maximal members of $\mathcal{C}_A(H)$. As $[\Gamma : H] = 7$, and $[N_A(\Delta) : H] = 3$, H is maximal in Γ and $N_A(\Delta)$. Therefore by Lemma 5.11 and (i) we have $\mathcal{M} = (\Gamma^S \cap \mathcal{C}_A(H)) \cup \{N_A(\Delta)\}$ and $\mathcal{C}_A(H) \cong M_{|\mathcal{M}|}$, so it remains to show that $|\Gamma^S \cap \mathcal{C}_A(H)| = 1$. Hence it suffices to show that if $\mathcal{B}' \subseteq \Omega$ and $(\Omega, \mathcal{B}')$ is the projective plane of order 2, then $\mathcal{B} = \mathcal{B}'$.

By (i), $C_H(\Delta) = O_2(H)$, the unique maximal normal 2-subgroup of H, and so $\Delta = \mathrm{Fix}(O_2(H))$. Let $\mathcal{I}$ be the set of involutions in $H - O_2(H)$. Let $B \in \mathcal{B} - \{\Delta\}$. By (i), $|N_H(B)| = 4$, so as $H \leqslant A$, H stabilizes Δ, and B contains a member of Δ, $N_H(B)$ is not trivial on B. Therefore, $|C_H(B)| = 2$, so $B = \mathrm{Fix}(i)$ for some $i \in \mathcal{I}$. As H acts on $\mathcal{B}$ and every member of $\mathcal{B}$ contains a member of Δ, we have $\mathrm{Fix}(i) \in \mathcal{B}$ for all $i \in \mathcal{I}$. Therefore, $\mathcal{B} = \{\mathrm{Fix}(O_2(H))\} \cup \{\mathrm{Fix}(i) : i \in \mathcal{I}\} = \mathcal{B}'$, and so the lemma holds. □

Lemma 7.9. *If $H = \Gamma_\omega$ for some projective semilinear* $\mathrm{P\Gamma L}_d(q) \cong \Gamma$ *and some $\omega \in \Omega$, and if $\mathcal{C}_A(H) \cong M_n$, then $n = 2$ or 3.*

Proof. If $d \geqslant 3$, then Γ is the automorphism group of a projective geometry over $\mathbb{F}_q$, so by the maximality of H in A_ω we have $H = N_{A_\omega}(\Sigma)$, where Σ is a partition of $\Omega - \{\omega\}$ into $(p-1)/q$ blocks each of size q, and in particular H stabilizes no other non-trivial partition of $\Omega - \{\omega\}$. On the other hand, if $d = 2$, then H is 2-transitive and hence primitive. Thus we conclude that if $H \leqslant \Gamma_2$ for some $\mathrm{P\Gamma L}_k(s) \cong \Gamma_2 \leqslant A$, then $(k, s) = (d, q)$.

Therefore, as Γ is 2-transitive, by Lemmas 5.4 and 5.11, we have

$$\mathcal{C}_A(H)' = \{A_\omega\} \cup (\Gamma^S \cap \mathcal{C}_A(H)).$$

So it remains to show that $|\Gamma^S \cap \mathcal{C}_A(H)| \leqslant 2$. This follows from Lemma 6.2 and the fact that $H = N_A(H)$ by the maximality of H in A_ω, so that

$$[N_S(H) : H] = [N_S(H) : N_A(H)] \leqslant 2. \quad \square$$

If V is a finite-dimensional vector space, and $\{V_i : 1 \leqslant i \leqslant n\}$ is a set of points of V (i.e. 1-dimensional subspaces of V), then we say that $V_1, \ldots, V_n$ are linearly

independent (respectively, linearly dependent) if $\dim(\sum_i V_i) = n$ (respectively, $\dim(\sum_i V_i) < n$).

Lemma 7.10. *If $H \leqslant A$ is intransitive, $H \leqslant \Gamma$ for some projective semilinear $\mathrm{P\Gamma L}_d(q) \cong \Gamma \leqslant A$, and $\mathcal{C}_A(H) \cong M_n$, then $n = 2$ or 3.*

Proof. By Lemma 5.1, Γ acts on Ω as on the points of the projective geometry $\mathrm{PG}(V)$. Let $d = \dim(V)$. By the maximality of H in Γ we have $H = N_\Gamma(B)$ for some non-empty set $B \subset \Omega$. Let Δ be the set of points in $\langle B \rangle$ and let e be the dimension of $\langle B \rangle$. Then as $H \leqslant N_\Gamma(\Delta)$, one of the following holds:

(I) $H = N_\Gamma(\Delta)$ and $\Delta \neq \Omega$ so that $e < d$;

(II) $\Delta = \Omega$ so that $e = d$.

Suppose that (I) holds. If $H^{\bar{\Delta}} \neq \mathrm{Sym}(\bar{\Delta})$, then by Lemma 7.1, we have $|\Delta| = 1$ and by Lemma 7.9, we have $n = 2$ or 3, so we may assume that $H^{\bar{\Delta}} = \mathrm{Sym}(\bar{\Delta})$. Let R be the unipotent radical of the parabolic subgroup H. Then

$$R \cong R^{\bar{\Delta}} \trianglelefteq H^{\bar{\Delta}} = \mathrm{Sym}(\bar{\Delta}),$$

so R is a non-trivial normal r-subgroup of $\mathrm{Sym}(\bar{\Delta})$, where $q = r^m$. Therefore $q^e(q^{d-e} - 1)/(q - 1) = |\bar{\Delta}| = 3$ or 4, so $(q^{d-e} - 1)/(q - 1) = 1$ and hence $d = e + 1$ and $(q, d) = (3, 2)$ or $(2, 3)$. But $(q, d) \neq (3, 2)$ as $(3^2 - 1)/(3 - 1) = 4$ is not prime, so $(q, d) = (2, 3)$ and by Lemmas 7.8 and 7.9, $n = 2$ or 3. Hence we may assume that (II) holds.

By symmetry between B and $\bar{B}$, we may assume that

(*) $\bar{B}$ has d linearly independent points.

Suppose that $d > 3$, and let V_1, V_2, V_3 be linearly independent points of B. Then $V_1 + V_2 + V_3$ has at least seven points, so by symmetry between B and $\bar{B}$, we may assume that $\bar{B}$ has four linearly dependent points, say V_4, V_5, V_6, V_7. As $d > 3$, by (*), $\bar{B}$ has four linearly independent points, say W_1, W_2, W_3, W_4. As Γ is projective semilinear, there is no member of Γ that maps $\{V_4, V_5, V_6, V_7\}$ onto $\{W_1, W_2, W_3, W_4\}$; so as $H = N_\Gamma(B)$, we have $H^{\bar{B}} \neq \mathrm{Sym}(\bar{B})$. Therefore by Lemma 7.1, $\mathcal{C}_A(H)$ is not an M-lattice, a contradiction. Therefore, either

(II)(A) $d = 3$, or

(II)(B) $d = 2$.

Suppose that (II)(A) holds. If $q > 3$, then any 2-dimensional subspace has at least six points, so we may assume that $\bar{B}$ has three linearly dependent points. Therefore, arguing as above, $H^{\bar{B}} \neq \mathrm{Sym}(\bar{B})$, and so by Lemma 7.1, $\mathcal{C}_A(H)$ is not an M-lattice, a contradiction. Therefore $q \leqslant 3$. If $q = 3$, then by (II)(A) we have $p = 13$ and $\Gamma \cong \mathrm{PGL}_3(3)$, so that $7! \nmid |\Gamma|$ and hence by Lemma 7.1, $\mathcal{C}_A(H)$ is not an M-lattice, a contradiction. Therefore $q = 2$ and by Lemmas 7.8 and 7.9, $n = 2$ or 3, so we may assume that (II)(B) holds. Thus

(**) $d = 2$, so $p = q + 1$ and hence by Lemma 5.3, q and m are powers of 2.

Assume without loss of generality that $|\bar{B}| \geqslant (p+1)/2$. By Lemma 7.9, we may assume that $|B| \geqslant 2$, so either

(i) $|B| \geqslant 3$, or

(ii) $|B| = 2$.

Suppose that (i) holds. Then by Lemma 7.1 we have $H^{\bar{B}} = \mathrm{Sym}(\bar{B})$, so as $|\bar{B}| \geqslant (p+1)/2$, by (**),

$$(q+2)/2 = (p+1)/2 \,|\, |\Gamma| = mqp(p-2),$$

q and m are powers of 2, and $(q+2)/2 = (p+1)/2 < p$. Thus as $(q+2)/2$ is odd we have $((q+2)/2, mqp) = 1$ and hence $(p+1)/2 \,|\, p-2$. Therefore, $(p+1)/2 = 3$, so $p = 7$ and $q = 6$, a contradiction. Hence we may assume that (ii) holds.

As Γ is 3-transitive, $N_A(B)$ is the unique maximal intransitive member of $\mathcal{C}_A(H)'$ and by Lemma 6.1, H is not contained in any affine subgroup of S. Hence by Lemmas 5.4 and 5.11, $\mathcal{C}_A(H)' \subseteq \Gamma^S \cup \{N_A(B)\}$, and it remains to show that $|\Gamma^S \cap \mathcal{C}_A(H)| \leqslant 2$. As $\mathcal{C}_A(H) \cong M_n$, H is maximal in $N_A(B)$, so that $H = N_A(H)$ and by Lemma 6.2, we have $|\Gamma^S \cap \mathcal{C}_A(H)| = [N_S(H) : N_A(H)] \leqslant 2$. □

Lemma 7.11. *If $H \leqslant G \cap A$ for some affine subgroup G of S and H is intransitive, then $\mathcal{C}_A(H)$ is not an M-lattice.*

Proof. Assume that $\mathcal{C}_A(H) \cong M_n$ for some $n \in \mathbb{N}$. By Lemma 6.1 and the maximality of H in $G \cap A$, we have $H = G_\omega \cap A$ for some $\omega \in \Omega$. As H is maximal in A_ω, $N_A(H) = H$, so as H is characteristic in G_ω, we obtain

$$|N_S(G_\omega)| \leqslant |N_S(H)| \leqslant 2|H| = |G_\omega|,$$

contrary to Lemma 6.3. □

Lemma 7.12. *For $n \in \mathbb{N}$, the following are equivalent:*

(1) *there exist a set Ω of prime order and $H \leqslant A = \mathrm{Alt}(\Omega)$ such that $\mathcal{C}_A(H) \cong M_n$;*

(2) $n \in \{1, 2, 3, 5, 7, 11\}$.

Proof. The implication (2) ⇒ (1) follows from Lemmas 6.5, 7.3 and 7.6.

(1) ⇒ (2) We may assume that $n \neq 1$ and by Lemmas 7.3 and 7.4, we may assume that $p \neq 11, 23$. Assume that H is contained in an affine subgroup G of S. Then by Lemma 7.11, H is transitive. If $p = 7$ or 17 then by Lemma 5.8 we have $G \cap A < \Gamma < A$, so as $\mathcal{C}_A(H) \cong M_n$, we have $H = G \cap A$. But then (2) holds by Lemma 6.5. Thus we may assume that $p \neq 7$ or 17, and then by Lemma 7.7 we may assume that H is not contained in a projective semilinear group. Therefore by Lemma 5.11, each maximal overgroup of H is affine. Thus $n = 1$ by Lemma 6.4, a contradiction. Therefore we may assume that H is not contained in any affine subgroup of S.

If H is transitive, then as $p \neq 11, 23$, by Lemma 5.9, H contains $G \cong \mathrm{PSL}_d(q)$, and by Lemmas 5.5 and 5.11, $N_A(G)$ is the unique maximal overgroup of H, so $n = 1$, a contradiction. Hence H is intransitive, so as H is not contained in any affine sub-

group of S and $p \neq 11, 23$, by Lemma 7.11, either $H = N_A(B) \cap N_A(C)$ for some non-empty sets $B, C \subset \Omega$ such that $C \notin \{B, \bar{B}\}$ or H is contained in a projective semilinear group of S. Thus (2) holds by Theorem 4.3 and Lemma 7.10. □

Lemma 7.13. *If $H \leqslant A$ and $\mathcal{O}_A(H) \cong M_2$, then one of the following holds:*

(1) *$H = N_\Gamma(B)$ for some projective semilinear $\Gamma \leqslant A$ and some proper non-empty subset B of Ω;*

(2) *$p \in \{7, 17, 23\}$ and $H = G \cap A$, where $G \leqslant S$ is affine.*

Proof. By Lemmas 7.3 and 7.4, we may assume that $p \neq 11, 23$. If H is intransitive, then as $\mathcal{O}_A(H) \cong M_2$, the subgroup H is not contained in an affine subgroup by Lemma 7.11, and H is not an intersection of two set stabilizers by 4.3. Hence by Lemma 5.11, H is contained in a projective semilinear subgroup Γ, so by the maximality of H in Γ, (1) holds. Hence we may assume that H is transitive.

If H is not contained in any affine subgroup of S, then as $p \neq 11, 23$ by Lemma 5.9, we have $\mathrm{PSL}_d(q) \leqslant H \leqslant \mathrm{P\Gamma L}_d(q)$, and so by Lemma 5.5, $\mathcal{O}_A(H)$ has exactly one maximal member, a contradiction.

Therefore H is contained in an affine subgroup of S, so by Lemma 7.7 we have $p = 7$ or 17. Thus by Lemma 6.4 we have $H \leqslant \Gamma \cong \mathrm{PSL}_3(2)$ or $\mathrm{P\Gamma L}_2(16)$. As H is maximal in Γ it follows that $H = G \cap A$, where $G = N_S(H)$ is affine, so (2) holds. □

Theorem 7.14. *For $H \leqslant A$, $\mathcal{O}_A(H)$ is not a $D\Delta(m_1, \ldots, m_t)$-lattice.*

Proof. Assume that $\mathcal{O}_A(H)$ is a $D\Delta(m_1, \ldots, m_t)$-lattice. First note that

(*) for each connected component $\Delta \cong \Delta(n)$ of $\mathcal{O}_A(H)$, there are $k_n = n(n-1)/2$ members of the third row of Δ and for each such member L, $\mathcal{O}_A(L) \cong M_2$.

Next we claim that

(**) H has at most two orbits on Ω.

To prove this, assume that H has more than two orbits on Ω. Then there exist non-empty sets $B, C \subset \Omega$ such that $B \notin \{C, \bar{C}\}$ and $H \leqslant K = N_A(B) \cap N_A(C)$. Let $P = P_{B,C}$. Now by Theorem 4.3, either $|P| = 4$ and $\mathcal{O}_A(K)$ is connected, or $|P| = 3$ and $\mathcal{O}_A(K)$ is isomorphic to M_3 or $M_2 * T_2$ or $M_4 * T_2$. The latter three cases do not occur by (*), so $|P| = 4$ and $\mathcal{O}_A(K)$ is connected.

Clearly $\mathcal{O}_A(K)$ has a member L in its third row, so by (*), we have $\mathcal{O}_A(L) \cong M_2$ and hence by Lemma 7.13, $\mathcal{O}_A(K)'$ has a transitive member. Therefore, by Lemmas 3.1 and 4.1, either P has type 2, 1^3 and $K = C_A(P) = 1$, or P has type 2^3, 1 and $|K| = 4$. Now the former case does not hold, because $H < K$ as $\mathcal{O}_A(H)$ is not connected. Therefore, P has type 2^3, 1, $|K| = 4$, and $H < K$.

Next note that for all non-empty sets $D, R \subset \Omega$ we have $|N_A(D) \cap N_A(R)| > 2$, so $H \neq N_A(D) \cap N_A(R)$, and hence the subposet consisting of the intransitive members of $\mathcal{O}_A(H)'$ is connected. But by Lemma 5.11, for any maximal transitive member $\Gamma \cong \mathrm{P\Gamma L}_3(2)$ of $\mathcal{O}_A(H)$, we have $H < \Gamma_\omega$ for some $\omega \in \Omega$, so $\mathcal{O}_A(H)$ is connected, a contradiction. Therefore, (**) holds.

Let $\Delta \cong \Delta(n)$ be a connected component of $\mathcal{C}_A(H)$, and let $L_1, \ldots, L_{k_n}$ be the members of the third row of Δ. Then by Lemma 7.13, (*) and (**), either

(I) for $1 \leqslant i \leqslant k_n$ we have $L_i = N_{\Gamma_i}(B)$ where $\Gamma_i \leqslant A$ is projective semilinear and $\varnothing \neq B \subset \Omega$, or

(II) $p = 7$ or 17 or 23 and for some $i \in \{1, \ldots, k_n\}$, $L_i = G \cap A$ where $G \leqslant S$ is affine.

If (I) holds, then $N_A(B)$ and $\Gamma_1, \ldots, \Gamma_{k_n}$ are $k_n + 1 > n$ distinct maximal members of Δ, a contradiction. Therefore (II) holds. If H is intransitive, then $H \leqslant G_\omega \cap A$ for some $\omega \in \Omega$ by Lemma 6.1, which contradicts (**). Therefore H is transitive, which contradicts Lemmas 6.4 and 7.13. □

Acknowledgement. The author would like to express his warm thanks to Professor Aschbacher for all his help with this paper.

References

[1] M. Aschbacher. *Sporadic groups* (Cambridge University Press, 1994).
[2] M. Aschbacher. Signalizer lattices in finite groups. (Preprint.)
[3] R. Baddeley and A. Lucchini. On representing finite lattices as intervals in subgroup lattices of finite groups. *J. Algebra* **196** (1997), 1–100.
[4] J. H. Conway. Three lectures on exceptional groups. In *Finite simple groups* (Academic Press, 1971), pp. 215–247.
[5] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker and R. A. Wilson. *Atlas of finite groups* (Clarendon Press, 1985).
[6] J. D. Dixon and B. Mortimer. *Permutation groups* (Springer-Verlag, 1996).
[7] D. Gorenstein, R. Lyons and R. Solomon. *The classification of the finite simple groups*, vol. 4 (American Mathematical Society, 1999).
[8] G. Grätzer. Two problems that shaped a century of lattice theory. *Notices Amer. Math. Soc.* **54** (2007), 696–707.
[9] R. M. Guralnick. Subgroups of prime power index in a simple group. *J. Algebra* **81** (1983), 304–311.
[10] P. Kleidman and M. Liebeck. *The subgroup structure of the finite classical groups* (Cambridge University Press, 1990).
[11] J. Kuan. Overgroups of intersections of maximal subgroups of the symmetric group. (Preprint.)
[12] M. W. Liebeck, C. E. Praeger and J. Saxl. A classification of the maximal subgroups of the finite alternating and symmetric groups. *J. Algebra* **111** (1987), 365–383.
[13] P. Palfy and P. Pudlak. Congruence lattices of finite algebras and intervals in the subgroup lattices of finite groups. *Algebra Universalis* **11** (1980), 22–27.
[14] K. Zsigmondy. Zur Theorie der Potenzreste. *Monatsh. Math. Phys.* **3** (1892), 265–284.

Received 10 December, 2007; revised 4 March, 2008

Philipp Perepelitsky, Department of Mathematics, California Institute of Technology, Pasadena, California, 91125, U.S.A.
E-mail: filipok@caltech.edu