TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 00, Number 0, Pages 000–000
S 0002-9947(XX)0000-0

EVERY COPRIME LINEAR GROUP ADMITS A BASE OF SIZE TWO

ZOLTÁN HALASI AND KÁROLY PODOSKI

Abstract. Let G be a linear group acting faithfully on a finite vector space V and assume that $(|G|, |V|) = 1$. In this paper we prove that G admits a base of size two and this estimate is sharp. This generalizes and strengthens several former results concerning base sizes of coprime linear groups. As a direct consequence, we answer a question of I. M. Isaacs in the affirmative.

1. Introduction

For a finite permutation group $H \leq \mathrm{Sym}(\Omega)$, a subset B of Ω is called a base if its pointwise stabilizer in H is the identity. There are a number of algorithms for permutation groups related to this concept, and these algorithms are faster if the size of the base is small. (As a reference for applications of small bases in computational group theory, see e.g. the book of Á. Seress [33].) Hence, for both practical and theoretical reasons it is important to find small bases for permutation groups. The base size of a permutation group H is defined as the smallest natural number $b(H)$ such that a base for H of size $b(H)$ exists. So, the best one may hope is to determine the base size of a permutation group. It is easy to see that

$$\frac{\log |H|}{\log |\Omega|} \leq b(H) \leq \log_2 |H|.$$

For primitive groups, L. Pyber [30, p. 207] asked whether the minimal base size is less than $c \log |H| / \log |\Omega|$ for some universal constant c. This needs to be verified for the various classes of primitive permutation groups that arise in the O'Nan–Scott theorem, and this problem has been investigated by several authors in recent years. An affirmative answer to Pyber's question was given by J. B. Fawcett [11] for diagonal groups and by T. C. Burness and Á. Seress [7] for product-type groups and for twisted wreath products. For almost simple groups, several papers could be mentioned, we just give here a few references. For standard actions, the existence of such constant c was proved by C. Benbenishty [2] (with $c < 15$). For non-standard actions, M. W. Liebeck and A. Shalev [23] proved that the base size is bounded by a constant. In fact, the optimal constant turns out to be 7, thanks to a series of papers of T. C. Burness et al. (see [3], [4], [5], [6]).

2010 *Mathematics Subject Classification.* Primary 20C15; Secondary 20B99.

Key words and phrases. coprime linear group, base size, regular partition .

The research leading to these results has received funding from the European Union's Seventh Framework Programme (FP7/2007-2013) under grant agreement no. 318202, from MTA Rényi Institute Lendület Limits of Structures Research Group, from ERC Limits of discrete structures Grant No. 617747 and from OTKA K84233.

So, the only primitive permutation groups for which Pyber's question is not solved yet are the affine primitive permutation groups. Even for these groups there are some partial results.

For example, the case where $H = V \rtimes G$ with G acting on the finite vector space V as a primitive linear group was solved by M. W. Liebeck and A. Shalev [24]. Furthermore, Á. Seress [31] proved that the minimal base size of any solvable primitive permutation group is at most four.

A linear group $G \leq GL(V)$ is called coprime if $(|G|, |V|) = 1$. If $G \leq GL(V)$ is such a group, then the affine group $H = V \rtimes G$ is called a coprime affine group. It turns out that the minimal base size of coprime affine groups is bounded. By a result of D. Gluck and K. Magaard [14] the minimal base size of any coprime affine group is at most 95. As $b(H) = b(G) + 1$ for an affine group H, this means that $b(G) \leq 94$ for any coprime linear group. Even for coprime nilpotent linear groups $G \leq GL(V)$, regular orbits on V do not always exist. (A description of all the possible coprime nilpotent linear groups without regular orbits is given by D. S. Passman [28]. As a concrete example, one can take the Sylow 3-subgroup of the group of monomial matrices in $GL(3, 4)$.) So the best one can hope for is that $b(G) \leq 2$ for any coprime linear group $G \leq GL(V)$, that is, $C_G(x) \cap C_G(y) = 1$ for some $x, y \in V$.

In the past, the existence of such a pair of vectors was confirmed for several special types of coprime linear groups such as for supersolvable groups (T. R. Wolf [35]), for groups of odd order (A. Moreto and T. R. Wolf [27]) and for solvable groups (S. Dolfi [10] and E. P. Vdovin [34]). In our paper we prove it without any additional conditions on G. Our main result is the following

Theorem 1.1. *Let V be a finite vector space and $G \leq GL(V)$ be a coprime linear group. Then $b(G) \leq 2$ for this action, i.e. there exist $x, y \in V$ such that $C_G(x) \cap C_G(y) = 1$.*

Using a lemma of B. Hartley and A. Turull [17, Lemma 2.6.2] one can obtain a more general corollary:

Corollary 1.2. *If G is a group acting faithfully on a group K and $(|G|, |K|) = 1$ then there exist $x, y \in K$ such that $C_G(x) \cap C_G(y) = 1$.*

As a direct consequence of Corollary 1.2 we have another proof of a theorem of P. P. Pálfy and L. Pyber.

Theorem 1.3 (P. P. Pálfy, L. Pyber [29, Theorem 1])**.** *If G is a group acting faithfully on a group K and $(|G|, |K|) = 1$ then $|G| < |K|^2$.*

There is a general consequence of Corollary 1.2, namely, in a faithful coprime action of a group G, there always exists an orbit of size at least $\sqrt{|G|}$. This answers a question raised by I. M. Isaacs [20].

Corollary 1.4. *If G is a group acting faithfully on a group K and $(|G|, |K|) = 1$ then there exists $x \in K$ such that $|C_G(x)| \leq \sqrt{|G|}$.*

Note that this corollary answers a special case of an important question of G. Malle and G. Navarro [25, Question 10.1] (with $P = 1$, in terms of their notation).

Finally, we note that in a very recent paper [16], a similar result to Theorem 1.1 has been obtained, by using the ideas and some partial results of this paper.

However, instead of the assumption that $G \leq GL(V)$ is coprime, this paper uses the weaker assumption that $G \leq GL(V)$ is p-solvable, where p denotes the characteristic of the base field of V. More precisely, the following has been proved.

Theorem 1.5 (Z. Halasi, A. Maróti [16, Theorem 1.1])**.** *Let V be a finite vector space over a field of order q and characteristic p. If $G \leq GL(V)$ is a p-solvable group with $O_p(G) = 1$, then $b(G) \leq 2$ unless $q \leq 4$. Moreover, if $q \leq 4$ then $b(G) \leq 3$.*

This paper is organized as follows. In Section 2 we investigate the following question: if G is a permutation group acting on Ω then, under some assumptions on G, at most how many parts must Ω be partitioned into such that only the identity element of G fixes every part of this partition? Using results of S. Dolfi [9] and Á. Seress [32], the main result of this section is Theorem 2.3. Using this theorem, we finish Section 2 by reducing Theorem 1.1 to primitive linear groups. In the following three sections we solve the problem for tensor product actions, for almost quasisimple groups and for groups of symplectic type by using results and methods from the papers of M. W. Liebeck and A. Shalev [24], and C. Köhler and H. Pahlings [22]. In the final section we prove Theorem 1.1 for arbitrary coprime linear groups by using induction on $\dim V$ and the results of the previous sections.

2. Regular partitions for permutation groups

Definition 2.1. Let Ω be a finite set and let $G \leq \mathrm{Sym}(\Omega)$ be a permutation group on Ω. A partition $\Omega = \cup_{i=1}^{t} \Omega_i$ is called G-regular, if $\cap_{i=1}^{t} G_{\Omega_i} = 1$, where G_X denotes the setwise stabilizer of X for any $X \subseteq \Omega$. In our terminology, empty sets as parts of a partition are allowed.

Remark 2.2. In the theory of permutation groups as well as in graph theory, this concept is sometimes referred to as a distinguishing partition, and the minimal number of parts t of a distinguishing partition is called the distinguishing number of the graph. Here, the distinguishing number is just the minimal number of colors needed to color the vertices of the graph in such a way that the colored graph has trivial automorphism group.

Theorem 2.3. *Let Ω be a finite set and let $G \leq \mathrm{Sym}(\Omega)$ be a permutation group such that G does not contain the alternating group $\mathrm{Alt}(t)$ as a section for some $t \geq 3$. Then there exists a G-regular partition of Ω with t parts.*

Proof. Our proof is based on a paper of S. Dolfi [9]. Following the notation of Dolfi, for every $s \in \mathbb{N},\ s \geq 2$ let

$$\mathscr{P}_s(\Omega) = \{(\Lambda_1, \Lambda_2, \ldots, \Lambda_s) \mid \Lambda_i \subseteq \Omega,\ \Lambda_i \cap \Lambda_j = \emptyset \text{ for } i \neq j,\ \cup_{i=1}^{s} \Lambda_i = \Omega\}$$

be the set of (ordered) partitions of Ω into s parts. (Note that our notation is not exactly the same as Dolfi's; the above set was denoted by $\mathscr{P}_{s-1}(\Omega)$ in Dolfi's paper.) Here the Λ_i's are allowed to be empty sets. Then G acts on $\mathscr{P}_s(\Omega)$ in a natural way for any s and we need to prove that G has a regular orbit on $\mathscr{P}_t(\Omega)$. We will use the following results proved by Dolfi:

(1) *If for some $t \in \mathbb{N}$ every primitive component (H, Δ) of G has at least t different regular orbits on $\mathscr{P}_t(\Delta)$, then G has a regular orbit on $\mathscr{P}_t(\Omega)$. (See* [9, Theorem 2]*.)*

(2) *If G has a regular orbit on $\mathscr{P}_s(\Omega)$ for some $s < t$, then G has at least t different regular orbits on $\mathscr{P}_t(\Omega)$. (Use* [9, Remark 2]*.)*

By using (1), we only need to prove that every primitive component (H, Δ) of G has at least t distinct regular orbits on $\mathscr{P}_t(\Delta)$. Noticing that H has a regular orbit on $\mathscr{P}_2(\Delta)$ if and only if there is a subset $X \subseteq \Delta$ such that the setwise stabilizer H_X of X in H is trivial we can use a result of Á. Seress [32, Theorem 2]. (See also [9, Theorem 1].) In Seress' paper, the primitive permutation groups (H, Δ) satisfying $H \not\geq \mathrm{Alt}(\Delta)$ and having no regular orbit on $\mathscr{P}_2(\Delta)$ have been determined using CFSG and the GAP system [12]. (We note that there is a small difference between the list of groups given by Seress and the list appearing in Dolfi's paper, since the latter assumes $H \not\geq \mathrm{Alt}(\Delta)$ only for $|\Delta| \geq 5$. In the following we use Dolfi's list.) If (H, Δ) has a regular orbit on $\mathscr{P}_2(\Delta)$, then it has at least t distinct regular orbits on $\mathscr{P}_t(\Delta)$ by using (2). If $H \geq \mathrm{Alt}(\Delta)$ but H does not contain $\mathrm{Alt}(t)$ as a section, then $|\Delta| < t$, so (H, Δ) has a regular orbit on $\mathscr{P}_s(\Delta)$ for $s = |\Delta| < t$, therefore, it has at least t distinct regular orbits on $\mathscr{P}_t(\Delta)$. Hence it remains to show that (H, Δ) has at least t regular orbits on $\mathscr{P}_t(\Delta)$ in case (H, Δ) is one of the 46 groups listed in [9, Theorem 1]. For these groups, the minimal value s for which H has a regular orbit on $\mathscr{P}_s(\Delta)$, along with their multiplicities, have been calculated by Dolfi (see [9, Lemma 1 a,c]). By using the GAP system [12] he proved that H has at least three regular orbits on $\mathscr{P}_3(\Delta)$ (hence it has at least t regular orbits on $\mathscr{P}_t(\Delta)$ for any $t \geq 3$) unless (H, Δ) is as in Table 1.

		Number of regular orbits		
H	$\lvert\Delta\rvert$	on $\mathscr{P}_3(\Delta)$	on $\mathscr{P}_4(\Delta)$	$\max\{t \mid \mathrm{Alt}(t)\ sec.\ H\}$
$\mathrm{Sym}(3)$	3	1	≥ 4	3
$PSL(2,5)$	6	1	≥ 4	5
$P\Gamma L(2,8)$	9	1	≥ 4	3
$\mathrm{Sym}(4)$	4	0	1	4
$PGL(2,5)$	6	0	≥ 4	5
$PSL(3,2)$	7	0	≥ 4	4
M_{11}	11	0	≥ 4	6
M_{12}	12	0	≥ 4	6
$ASL(3,2)$	8	0	1	4

TABLE 1. Primitive groups with fewer than three regular orbits on $\mathscr{P}_3(\Delta)$.

The first four columns of this table collect the results of the above mentioned lemma of Dolfi. For each of these groups H, we calculated the largest t such that H contains the alternating group $\mathrm{Alt}(t)$ as a section. The last column of Table 1 contains this information.

For $t = 3$, we deduce that (H, Δ) cannot be any of these primitive permutation groups. For $t = 4$, the only possibilities for H are $\mathrm{Sym}(3)$ and $P\Gamma L(2,8)$ but in these cases there are at least 4 regular orbits on $\mathscr{P}_4(\Delta)$. Finally, for $t \geq 5$ each of these primitive permutation groups has at least t regular orbits on $\mathscr{P}_t(\Delta)$. □

Corollary 2.4. *Let $t \geq 2$ be an integer and let us assume that $G \leq \mathrm{Sym}(\Omega)$ with $t \nmid |G|$. Then there exists a G-regular partition of Ω with t parts.*

Proof. For $t = 2$ we have that G is a group of odd order, hence there is a G-regular partition of Ω with 2 parts by a result of D. Gluck [13, Corollary 1]. Otherwise, if $t \nmid |G|$, then G cannot contain $\mathrm{Alt}(t)$ as a section, so there is a G-regular partition of Ω with t parts by Theorem 2.3. □

Remark 2.5. Without using CFSG, it can be shown that if G is a permutation group on Ω such that no $g \in G$ contains a cycle of length greater than t, then there is a G-regular partition of Ω with t parts.

By using Corollary 2.4, we close this section by reducing Theorem 1.1 to primitive linear groups. We remind the reader that a linear group $H \leq GL(V)$ is primitive if there is no nontrivial direct sum decomposition $V = V_1 \oplus V_2 \oplus \ldots \oplus V_k$ such that every element of H permutes the subspaces $V_1, V_2, \ldots, V_k$. Note that primitivity implies irreducibility, i.e. if V is a finite vector space over the finite field $\mathbb{F}_q$ and $H \leq GL(V)$ is a coprime primitive linear group, then V is an irreducible $\mathbb{F}_q H$-module.

Theorem 2.6. *Let us assume that $b(H) \leq 2$ for any finite vector space W and for any coprime primitive linear group $H \leq GL(W)$. Then $b(G) \leq 2$ for any finite vector space V and for any coprime linear group $G \leq GL(V)$.*

Proof. Let $G \leq GL(V)$ be any coprime imprimitive linear group acting on V, where V is a finite vector space over the finite field $\mathbb{F}_q$ of characteristic p. By Maschke's theorem, V is completely reducible as a $\mathbb{F}_q G$-module. If V is not irreducible as a $\mathbb{F}_q G$-module, then $V = V_1 \oplus V_2$ for some proper G-invariant subspaces $V_1, V_2 \leq V$. By using induction on $\dim V$, for $i = 1, 2$ set $x_i, y_i \in V_i$ such that $C_G(x_i) \cap C_G(y_i) = C_G(V_i)$. Then $C_G(x_1 + x_2) \cap C_G(y_1 + y_2) = C_G(V_1) \cap C_G(V_2) = 1$.

For the remainder let $G \leq GL(V)$ be an irreducible, imprimitive linear group. Thus, there is a decomposition $V = \oplus_{i=1}^{k} V_i$ such that $k \geq 2$ and G permutes the subspaces V_i in a transitive way. We can assume that the decomposition cannot be refined. For each $1 \leq i \leq k$ let $H_i = \{g \in G \mid gV_i = V_i\}$ be the stabilizer of V_i in G. Then $H_i / C_{H_i}(V_i) \leq GL(V_i)$ is a primitive linear group, and the subgroups H_i are conjugate in G. Of course, $(|H_1|, |V_1|) = 1$, so, by using the hypothesis, we can find vectors $x_1, y_1 \in V_1$ such that $C_{H_1}(x_1) \cap C_{H_1}(y_1) = C_{H_1}(V_1)$. Let

$$\{g_1 = 1, g_2, \ldots, g_k\} \tag{D.1}$$

be a set of left coset representatives for H_1 in G such that $V_i = g_i V_1$ for all $1 \leq i \leq k$ and let $x_i = g_i x_1$, $y_i = g_i y_1$. It is clear that $H_i = H_1^{g_i^{-1}}$ and $C_{H_i}(x_i) \cap C_{H_i}(y_i) = C_{H_i}(V_i)$.

Now, $N = \cap_{i=1}^{k} H_i$ is a normal subgroup of G, the quotient group G/N acts faithfully and transitively on the set $\Omega = \{V_1, V_2, \ldots, V_k\}$, and $|G/N|$ is coprime to p. Using Corollary 2.4, there is a G/N-regular partition of Ω into p parts, say, $\Omega = \Lambda_1 \cup \ldots \cup \Lambda_p$. Then we can choose a vector $(a_1, a_2, \ldots, a_k) \in \mathbb{F}_p^k$ such that $a_i = a_j$ if and only if V_i and V_j are in the same part of the partition $\Omega = \Lambda_1 \cup \ldots \cup \Lambda_p$. Now, let the vectors $x, y \in V$ be defined as

$$x = \sum_{i=1}^{k} x_i, \qquad y = \sum_{i=1}^{k} (y_i + a_i x_i).$$

We claim that $C_G(x) \cap C_G(y) = 1$. Let $g \in C_G(x) \cap C_G(y)$. Assuming that $gV_i = V_j$ for some $1 \leq i, j \leq k$ we get $gx_i = x_j$ and $g(y_i + a_i x_i) = (y_j + a_j x_j)$. Let

$g' = g_j^{-1} g g_i \in G$ where the g_i are the elements given in D.1. Then

$$g'x_1 = x_1 \quad \text{and} \quad g'(y_1 + a_i x_1) = (y_1 + a_i x_1) + (a_j - a_i)x_1, \tag{D.2}$$

so g' stabilizes the subspace $\langle x_1, y_1 \rangle \leq V_1$. If $y_1 = cx_1$ for some $c \in \mathbb{F}_p$, then $g'y_1 = y_1$, and using Equation (D.2) we get $a_j = a_i$. Otherwise, $x_1, y_1 + a_i x_1$ form a basis of the $\langle g' \rangle$-invariant subspace $\langle x_1, y_1 \rangle$. With respect to this basis the restriction of g' to this subspace has matrix form

$$\begin{pmatrix} 1 & a_j - a_i \\ 0 & 1 \end{pmatrix}.$$

If $a_j - a_i \neq 0$, then this matrix has order p, so p divides the order of $g' \in G$, a contradiction. Hence in any case $a_i = a_j$ holds for $gV_i = V_j$, which exactly means that $gN \in G/N$ stabilizes the vector $(a_1, a_2, \ldots, a_k)$. It follows that $g \in N$. So $gx_i = x_i$ and $gy_i = y_i$ holds for any $1 \leq i \leq k$, and $g \in \cap_{i=1}^{k} C_{H_i}(V_i) = C_G(V) = 1$ follows. □

Having now reduced the problem to the case when $G \leq GL(V)$ acts primitively on V, we now give a brief description of our strategy for the proof of Theorem 1.1.

For the remainder, let $\mathbb{F}_q$ be the base field of V and let $Z \leq GL(V)$ be the group of scalar transformations, so $Z \simeq \mathbb{F}_q^\times$. It is clear that $G \leq GZ \leq GL(V)$ and $|GZ|$ divides $|G|(q-1)$, so GZ is a coprime linear group containing G. It is clear that $b(G) \leq b(GZ)$. Therefore, in order to prove Theorem 1.1 we can (and we will) assume without loss of generality that G contains Z.

Now, let $Z \leq N \lhd G \leq GL(V)$ be a minimal normal subgroup of G above Z, i.e. N/Z is a minimal normal subgroup of G/Z. Assuming that V is an absolutely irreducible $\mathbb{F}_q N$-module, we distinguish three subcases:

(a) N/Z is a proper direct power of a non-abelian simple group;
(b) N/Z is itself a non-abelian simple group;
(c) N/Z is an elementary abelian r-group for some prime r.

In Section 3 we reduce case (a) to case (b), which will be settled in Section 4. Then we handle case (c) in Section 5. Finally, we finish the proof of Theorem 1.1 in Section 6 by using an induction argument in case of the action of N on V is not absolutely irreducible.

3. Tensor product actions

The purpose of this section is to find a base for linear groups acting on tensor product spaces. Before going into details, we first prove a lemma about strong bases, which says that during our proof we can always use the more specific concept of strong base instead of the concept of base. The reason of this method is that at some points of the proof it is easier to do the induction step by using strong bases instead of arbitrary bases.

We start this section with the definition of strong base and strong base size introduced in [24].

Definition 3.1. For a linear group $G \leq GL(V)$ a strong base for G is a set $B \subseteq V$ of vectors such that any element $g \in G$ fixing $\langle v \rangle$ for every $v \in B$ is a scalar matrix. The minimal size of a strong base for G is called the strong base size, denoted by $b^*(G)$.

Remark 3.2. It was proved by Liebeck and Shalev [24, Lemma 3.1] that $b(G) \leq b^*(G) \leq b(G)+1$ for any linear group $G \leq GL(V)$.

For the base sizes and strong base sizes of coprime linear groups we have the following.

Lemma 3.3. *Let $G \leq GL(V)$ be a coprime linear group containing Z with a two-element base $u_1, u_2 \in V$. Then $u_1,\ u_1+\gamma u_2$ is a strong base for some $\gamma \in \mathbb{F}_q$.*

Proof. The case when u_1 and u_2 are linearly dependent is trivial, since a one-element base for a linear group containing Z is always a strong base for G. Now, let $u_1,\ u_2$ be linearly independent vectors. Then $u_1, u_1+\alpha u_2$ is also a base for G for every $\alpha \in \mathbb{F}_q^\times$. For $\alpha \in \mathbb{F}_q^\times$ let

$$X_\alpha = \{\lambda \in \mathbb{F}_q^\times \setminus \{1\} \mid \exists\, g \in G; gu_1 = u_1,\, g(u_1+\alpha u_2) = \lambda(u_1+\alpha u_2)\}.$$

We claim that $X_\alpha \cap X_\beta = \emptyset$ if $\alpha \neq \beta$ are non-zero field elements. Indeed, let us assume that $\lambda \in X_\alpha \cap X_\beta$. Then there exist $g, h \in G$ such that

$$\begin{matrix} gu_1 = u_1 \\ g(u_1+\alpha u_2) = \lambda(u_1+\alpha u_2) \end{matrix} \quad \text{and} \quad \begin{matrix} hu_1 = u_1 \\ h(u_1+\beta u_2) = \lambda(u_1+\beta u_2) \end{matrix}.$$

Then both g and h fix the two dimensional subspace $U = \langle u_1, u_2\rangle$. The restrictions of g and h to this subspace have the following matrix forms:

$$g_U = \begin{pmatrix} 1 & (\lambda-1)/\alpha \\ 0 & \lambda \end{pmatrix} \qquad \text{and} \qquad h_U = \begin{pmatrix} 1 & (\lambda-1)/\beta \\ 0 & \lambda \end{pmatrix}.$$

Thus, $g_U^{-1}h_U$ is an upper unitriangular matrix different from 1_U, hence $o(g^{-1}h)$ is divisible by $p = o(g_U^{-1}h_U)$, a contradiction.

Using the pigeonhole principle, it follows that $X_\gamma = \emptyset$ for some $\gamma \in \mathbb{F}_q^\times$. Let $v_1, v_2 \in V$ be defined as $v_1 = u_1$ and $v_2 = u_1 + \gamma u_2$. Let us assume that $g \in G$ fixes both $\langle v_1\rangle$ and $\langle v_2\rangle$ and let $\lambda_1, \lambda_2 \in \mathbb{F}_q^\times$ be such that $gv_1 = \lambda_1 v_1,\ gv_2 = \lambda_2 v_2$. As G contains every non-zero scalar matrix, $g_0 = \lambda_1^{-1} g \in G$. Now, g_0 fixes v_1 and moves v_2 by a scalar multiple. Using the definition of γ, we get $g_0 v_2 = v_2$. As v_1, v_2 is also a base for G, it follows that $g_0 = 1$, that is, g is a scalar matrix. Hence v_1, v_2 is a strong base for G. □

For the remainder of this section, let V_1 be an $m \geq 2$ dimensional vector space over the field $\mathbb{F}_q$, and let $\{x_1, x_2, \ldots, x_m\} \subseteq V_1$ be a basis of V_1. For any k and $1 \leq i \leq m$ let the vector space $V_1^{(k)}$ and $x_i^{(k)} \in V_1^{(k)}$ be defined as

$$V_1^{(k)} := \underbrace{V_1 \otimes \cdots \otimes V_1}_{k \text{ factors}}, \qquad x_i^{(k)} := \underbrace{x_i \otimes \cdots \otimes x_i}_{k \text{ factors}}.$$

Furthermore, let $V = V_1^{(t)}$ and let

$$B = \underbrace{GL(V_1) \otimes \cdots \otimes GL(V_1)}_{t \text{ factors}} = \{A_1 \otimes \cdots \otimes A_t \mid A_1, \ldots, A_t \in GL(V_1)\} \leq GL(V)$$

acting on V with its natural tensor product action, that is, for elements $v_1, \ldots, v_t \in V_1$ and $A_1, \ldots, A_t \in GL(V_1)$ we have

$$(A_1 \otimes \cdots \otimes A_t)(v_1 \otimes \cdots \otimes v_t) = (A_1 v_1 \otimes \cdots \otimes A_t v_t)$$

Note that as an abstract group, B is just the t-th central power of $GL(V_1)$, but we would like to emphasize its tensor product action, so we use the notation $\otimes$ instead of $\star$, which is the notation we will use in Section 4 for central products.

In this section we are interested in groups $G \leq GL(V)$, where $V = V_1^{(t)}$ and G preserves the tensor product decomposition. This means that $G \leq B \rtimes S_t$, where B is as above, while S_t acts by permuting the factors of the tensor product decomposition $V = V_1 \otimes \cdots \otimes V_1$. With this notation we have the following.

Lemma 3.4. *Let V_1 be a vector space over $\mathbb{F}_q$ with basis $\{x_1, \dots, x_m\} \subseteq V_1$, and let $t \geq 2$. Then the group $B = \underbrace{GL(V_1) \otimes \cdots \otimes GL(V_1)}_{t \text{ factors}}$ acts in the natural way on $V = V_1^{(t)}$. Let $x = \sum_{i=1}^m x_i^{(t)} \in V$. Then the matrix form of $C_B(x)$ with respect to the lexicographically ordered basis $\{u_1 \otimes \cdots \otimes u_t \,|\, u_i \in \{x_1, \dots, x_m\}\ \forall 1 \leq i \leq t\}$ is the following.*

1. *For $t = 2$ we have $C_B(x) = \{A \otimes A^{-T} \,|\, A \in GL(m, q)\}$.*
2. *For $t \geq 3$ let $P \leq GL(m, q)$ be the group of permutation matrices and $D \leq GL(m, q)$ be the group of diagonal matrices with respect to the basis $\{x_1, \dots, x_m\}$. Then*

$$C_B(x) = \left\{ A_1 S \otimes \cdots \otimes A_t S \,|\, S \in P,\ A_1, \dots, A_t \in D,\ A_1 \cdots A_t = I \right\}.$$

Proof. For $t = 2$ let $A_1 = (\alpha_{ij}),\ A_2 = (\beta_{ij}) \in GL(m, q)$ with $A_1 \otimes A_2 \in C_B(x)$. As the coefficient of $x_i \otimes x_j$ in $(A_1 \otimes A_2)(x_k \otimes x_k)$ is $\alpha_{ik}\beta_{jk}$, it follows that

$$\sum_{k=1}^m (A_1 \otimes A_2)(x_k \otimes x_k) = \sum_{k=1}^m (x_k \otimes x_k) \iff \sum_{k=1}^m \alpha_{ik}\beta_{jk} = \delta_{ij} \text{ for all } 1 \leq i, j \leq m.$$

This exactly means that $A_1 A_2^T = I$, which proves part (1).

Now assume $t \geq 3$. Let $M_1 \otimes \cdots \otimes M_t \in C_B(x)$ for some $M_1, M_2, \dots, M_t \in GL(m, q)$. By using [24, Lemma 3.3 (i)] for

$$W_2 := \langle x_1^{(2)}, \dots, x_m^{(2)} \rangle, \quad W_{t-2} := \langle x_1^{(t-2)}, \dots, x_m^{(t-2)} \rangle$$

and for the decomposition $x = \sum_{i=1}^m x_i^{(2)} \otimes x_i^{(t-2)}$ we get that $(M_1 \otimes M_2)(x_j^{(2)}) \in W_2$ for every $1 \leq j \leq m$. In this product the coefficient of $x_k \otimes x_l$ is $\alpha_{kj}\beta_{lj}$ where $M_1 = (\alpha_{ij}),\ M_2 = (\beta_{ij})$. So $\alpha_{kj}\beta_{lj} = 0$ unless $k = l$. If $\alpha_{kj} \neq 0$ for some k then $\beta_{lj} = 0$ for every $l \neq k$ and $\beta_{kj} \neq 0$. Reversing the role of α and β and applying this argument for every $1 \leq j \leq m$, it follows that both M_1 and M_2 are monomial matrices with the same permutation part. Of course, all of this can be said for every pair of matrices $M_i,\ M_j$ with $1 \leq i \neq j \leq t$, which proves that

$$C_B(x) \subseteq \left\{ A_1 S \otimes \cdots \otimes A_t S \,|\, S \in P,\ A_1, \dots, A_t \in D \right\}.$$

If $M = A_1 S \otimes \cdots \otimes A_t S \in C_B(x)$ for some $S \in P$ and $A_1, \dots, A_t \in D$, then the i-th entry of the main diagonal of $A_1 \cdots A_t \in D$ is the coefficient of $x_i^{(t)}$ in Mx, which is 1. This proves that $C_B(x)$ is contained in the set given in part (2) of the statement. The proof of the converse containment is an obvious calculation. □

Remark 3.5. We note that in case $t = 2$ this result was essentially proved in the proof of [24, Lemma 3.3 (iii)], while in case $t \geq 3$ there is an incorrect description of this centralizer in the proof of [24, Lemma 3.5].

Theorem 3.6. *Let V_1 be a vector space over $\mathbb{F}_q$ of dimension $d \geq 2$ and let $Z \leq G_1 \leq GL(V_1)$ be any linear group such that $b^*(G_1) \leq 2$. For any $t \geq 2$ let $G = G_1 \wr_c S_t$ be the central wreath product of G_1 by S_t, that is, G is a split extension of the base group $B = \underbrace{G_1 \otimes \cdots \otimes G_1}_{t \text{ factors}}$ by S_t. Then G acts faithfully on the tensor power $V = V_1^{(t)}$ in a natural way, so it is embedded into $GL(V)$. If $(d,t) \neq (2,2)$ then $b(G) \leq 2$ with respect to the action of G on V.*

Proof. Let $x_1, y_1 \in V_1$ be a strong base for G_1 such that x_1, y_1 are linearly independent and let $U_1 = \langle x_1, y_1 \rangle$. Let $x = x_1^{(t)} + y_1^{(t)}$. As S_t acts on the tensor product by permuting factors, we clearly have $S_t \leq C_G(x)$, hence $C_G(x) = H \rtimes S_t$ for the subgroup $H = C_B(x)$. Let $h_1 \otimes \cdots \otimes h_t \in H$ be any element of H. (Note that $h_1, \ldots, h_t \in G_1$ are only defined up to scalars.) Applying [24, Lemma 3.3(i)] for V_1 and $V_1^{(t-1)}$ it follows that $U_1 \leq V_1$ is fixed by $h_1 \in G_1$. Since S_t acts by conjugation on H and it permutes its coordinates in a transitive way we get that U_1 is h_i-invariant for all $1 \leq i \leq t$, so $U = U_1^{(t)} \leq V_1^{(t)}$ is $C_G(x)$-invariant. Therefore, H fixes the subspace U. Let $H|_U$ denote the restriction of the action of H to U. By Lemma 3.4, the matrix form of $H|_U$ is the following:

- If $t = 2$ we have $H|_U \subseteq \{A \otimes A^{-T} \mid A \in GL(2,q)\}$.
- If $t \geq 3$

$$H|_U \subseteq \left\{ A_1 S^\varepsilon \otimes \cdots \otimes A_t S^\varepsilon \mid \varepsilon \in \{0,1\}, A_i = \begin{pmatrix} \lambda_i & 0 \\ 0 & \mu_i \end{pmatrix}, \prod_i \lambda_i = \prod_i \mu_i = 1 \right\},$$

where $S = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in GL(2,q)$.

Now, we define $y \in V_1^{(t)}$ such that $C_G(x) \cap C_G(y) = 1$. First, let us assume that $t = 2$. Since $\dim V_1 = d \geq 3$ by our assumption, let $z_1 \in V_1 \setminus U_1$. Let $y \in V_1^{(2)}$ be defined as

$$y = x_1 \otimes z_1 + y_1 \otimes x_1.$$

Let us assume that $g \in C_G(x) \cap C_G(y)$. Then $g = h\sigma$, where $h = h_1 \otimes h_2 \in H$ for some $h_1, h_2 \in G_1$ and $\sigma \in S_2$. Furthermore, h fixes $U = U_1 \otimes U_1$ and $h|_U = A \otimes A^{-T}$ for some $A \in GL(2,q)$. If $\sigma \neq 1$, then $gy \in V_1 \otimes U_1$, while $y \notin V_1 \otimes U_1$, a contradiction. Thus, $g = h$ and $gy \in Ax_1 \otimes V_1 + Ay_1 \otimes A^{-T}x_1$. Extend $x_1 \otimes z_1, y_1 \otimes x_1, y_1 \otimes z_1, y_1 \otimes y_1$ to a basis of V and write $gy = y$ as a linear combination of the basis elements. Comparing the coefficients of the basis elements, we get that $g(x_1 \otimes z_1)$ contains $x_1 \otimes z_1$ with non-zero coefficient, while the coefficient of $y_1 \otimes z_1$ in $g(x_1 \otimes z_1)$ is zero. It follows that x_1 is an eigenvector of A. Now, $Ay_1 \otimes A^{-T}x_1$ contains $y_1 \otimes x_1$ with non-zero coefficient, while the coefficient of $y_1 \otimes y_1$ in $Ay_1 \otimes A^{-T}x_1$ is zero. It follows that x_1 is an eigenvector of A^{-T} too. Therefore, A is a diagonal matrix. Since $h_1|_{U_1} = A, h_2|_{U_1} = A^{-T}$ and we chose x_1, y_1 to be a strong base for G_1, it follows that $h_1, h_2 \in Z$. Hence $g = h_1 \otimes h_2 = 1$.

For $t \geq 3$ let $y \in V$ be defined as

$$y = x_1^{(t)} + \sum_{i=1}^{t-1} x_1^{(t-i)} \otimes y_1^{(i)}.$$

Now, if $g = h\sigma \in C_G(x) \cap C_G(y)$, where $h = h_1 \otimes h_2 \otimes \cdots \otimes h_t \in H$ for some $h_1, \ldots, h_t \in G_1$ and $\sigma \in S_t$ then h leaves invariant U and $h|_U = A_1 S^\varepsilon \otimes \cdots \otimes A_t S^\varepsilon$.

Now, if $\varepsilon = 1$, then y contains $x_1^{(t)}$ with non-zero coefficient, while gy does not, a contradiction. It follows that $h|_U = A_1 \otimes \cdots \otimes A_t$.

As $h_i|_{U_1} = A_i$ is a diagonal matrix with respect to the basis $x_1, y_1 \in U_1$ and x_1, y_1 is a strong base for $G_1 \leq GL(V_1)$ we get that $h_i \in Z$ for every $1 \leq i \leq t$. It follows that $h = 1$ and $g = \sigma \in S_t$. If $\sigma(i) = j$ for some $i < j$, then y contains $x_1^{(i)} \otimes y_1^{(t-i)}$ with non-zero coefficient, while gy does not, which proves that $g = 1$, as claimed. □

Remark 3.7. The assumption $(d, t) \neq (2, 2)$ is crucial in the previous theorem. By taking $V_1 \simeq \mathbb{F}_3^2$ and $G_1 = SL(V_1) \geq Z$ we get $b^*(G_1) = b(G_1) = 2$, while the base size of $G = (G_1 \otimes G_1) \rtimes S_2$ acting on $V_1 \otimes V_1$ is 3.

Theorem 3.8. *Let V_1 be a finite vector space over $\mathbb{F}_q$ of dimension $d \geq 2$ and let $Z \leq G_1 \leq GL(V_1)$ be a coprime linear group with $b(G_1) \leq 2$. Furthermore, let $G \leq G_1 \wr_c S_t \leq GL(V)$ be a coprime linear group acting on $V = V_1^{(t)}$, where $t \geq 2$. Then $b(G) \leq 2$ for this action.*

Proof. By Lemma 3.3, we have $b^*(G_1) \leq 2$. Therefore, we can apply Theorem 3.6 to conclude that $b(G) \leq 2$ unless $(d, t) = (2, 2)$.

For $(d, t) = (2, 2)$ let $\{x_1, x_2\} \subseteq V_1$ be a strong base for G_1, let $\sigma \in S_2$, $\sigma \neq 1$ and let $\alpha \in \mathbb{F}_q^\times$ be a generator of the multiplicative group of $\mathbb{F}_q$. For q even, we have $G \leq G_1 \otimes G_1$ since $(|G|, |V|) = 1$, so $b(G) \leq b^*(G) \leq b^*(G_1) \leq 2$ holds by [24, Lemma 3.3 (ii)]. Therefore, we may assume that q is odd. We assume by way of contradiction that there is no $u, v \in V$ such that $C_G(u) \cap C_G(v) = 1$. Let $u_i = x_i \otimes x_i$, $v_i = x_i \otimes x_{3-i} + \alpha x_{3-i} \otimes x_i$ for $i \in \{1, 2\}$. An easy calculation shows that there exist $c_1, c_2 \in \mathbb{F}_q^\times$ such that

$$1 \neq g_1 \in C_G(u_1) \cap C_G(v_1) \iff g_1 = (a_1 \otimes a_1^{-1})\sigma \text{ where } a_1 = \begin{pmatrix} 1 & c_1 \\ 0 & \alpha \end{pmatrix},$$

$$1 \neq g_2 \in C_G(u_2) \cap C_G(v_2) \iff g_2 = (a_2 \otimes a_2^{-1})\sigma \text{ where } a_2 = \begin{pmatrix} 1 & 0 \\ c_2 & \alpha \end{pmatrix}.$$

Now, $H = \langle a_1, a_2, Z \rangle \leq G_1$. Defining $H_1 = \langle a_1, Z \rangle$ and $H_2 = \langle a_2 \rangle$ we get $|H_1| = (q-1)^2$, $|H_2| = q - 1$ and $H_1 \cap H_2 = 1$. Therefore, $|H| \geq |H_1 H_2| = |H_1||H_2| = (q-1)^3$. As $(|H|, q) = 1$, and $|H|$ divides $|GL(2, q)| = q(q+1)(q-1)^2$, it follows that H is a q'-Hall subgroup of $GL(V_1)$, in particular $|GL(V_1) : H| = q$. This means that $PSL(2, q)$ contains a subgroup of index q which is impossible by [21, Table 5.2.A] unless $q \in \{3, 5, 7, 9, 11\}$. The remaining cases were checked using GAP [12]. □

4. Almost quasisimple groups

In this section we suppose that p is a prime, V is an n-dimensional vector space over $\mathbb{F}_p$ and $G \leq GL(V)$ is a p'-group having a quasisimple irreducible normal subgroup N. In order to prove the existence of a base of size two for such a group, we use a result of C. Köhler and H. Pahlings [22]. By using D. P. M. Goodwin's theorem [15], they proved that there exists a regular orbit for such a group in most cases and they gave a description of the exceptions (see Table 2) with the isomorphism type of a stabilizer of a vector having smallest order. Using this result, for these linear groups we choose an $x \in V$ such that $|C_G(x)|$ is as small as possible and we prove the existence of a vector $y \in V$ such that $C_G(x) \cap C_G(y) = 1$.

Theorem 4.1 (D. P. M. Goodwin [15], C. Köhler and H. Pahlings [22])**.** *Suppose p is a prime, V is an n-dimensional vector space over $\mathbb{F}_p$ and $G \leq GL(V)$ is a p'-group having a quasisimple normal subgroup N which is irreducible on V. If G has no regular orbit on the vectors of V, then one of the following holds:*

(1) *$N = \mathrm{Alt}(c)$, the alternating group of degree c for $c < p$ and V is the deleted permutation module for N of dimension $c - 1$.*
(2) *G, n, p are as in Table 2.*

G	n	p	*minimal stabilizer*
$\mathrm{Alt}(5) \times Z$	3	11	C_2
$\mathrm{Alt}(5).2 \times Z$	4	7	C_2
$2.\mathrm{Alt}(5) \star Z$	2	$29, 41, 61, 11, 19, 31$	$C_2, C_2, C_2, C_5, C_3, C_3$
$Z.(8 \star 2.\mathrm{Alt}(5)).2$	4	7	V_4
$\mathrm{Alt}(6).2 \times Z$	5	7	C_2
$2.\mathrm{Alt}(6).2 \star Z$	4	7	C_3
$3.\mathrm{Alt}(6) \star Z$	3	$19, 31$	C_2, C_2
$2.\mathrm{Alt}(7) \star Z$	4	11	C_3
$L_2(7) \times Z$	3	11	C_2
$Z.(6 \times L_2(7)).2$	6	5	C_2
$U_3(3) \times Z$	7	5	C_2
$U_3(3).2 \times Z$	7	5	C_2
$(U_3(3) \times Z).2$	6	5	S_3
$U_4(2) \times Z$	5	$7, 13, 19$	S_4, V_4, C_2
$U_4(2).2 \times Z$	6	$7, 11, 13$	D_{12}, V_4, C_2
$2.U_4(2) \star Z$	4	$7, 13, 19, 31, 37$	$U_{72}, U_{18}, (C_3^2, C_9), C_3, C_2$
$6_1.U_4(3).2_2 \star Z$	6	$13, 19, 31, 37$	$W(B_3), S_3 \times C_2, V_4, C_2$
$U_5(2) \times Z$	10	7	V_4
$Sp_6(2) \times Z$	7	$11, 13, 17, 19$	C_2^3, V_4, C_2, C_2
$2.\Omega_8^+(2) \star Z$	8	$11, 13, 17, 19, 23$	$W(B_3), S_4, S_3, V_4, C_2$
$2.J_2 \star Z$	6	11	S_3

TABLE 2. Coprime linear groups of quasisimple type with no regular orbit

Remark 4.2. In the above table, the first column records the largest possible group G. Furthermore, $Z \simeq (\mathbb{F}_p)^\times$, while $\star$ denotes the central product of groups. In the column headed by "minimal stabilizer" the isomorphism type of a stabilizer of a vector having smallest order is displayed. It is always unique, unless $G = 2.U_4(2) \star Z$ and $(n, p) = (4, 19)$, where there are two such types. U_{72}, U_{18} are certain subgroups of $U_4(2)$ of order 72 and 18 respectively. Finally, $V_4 = C_2 \times C_2$ and $W(B_3) = S_4 \times C_2$ denote the Klein 4-group and the Weyl group of the root system B_3, respectively.

For $g \in G$, let $C_V(g) \leq V$ denote the fixed point space of g. We can naturally define $C_V(H) = \cap_{h \in H} C_V(h)$ for each $H \subset G$. By choosing an $x \in V$ such that $C_G(x)$ is isomorphic to the minimal stabilizer, we prove that if $H_1, H_2, \ldots, H_t$ are the minimal subgroups of $C_G(x)$ then $\cup_i C_V(H_i) \neq V$. Consequently, for any $y \in V \setminus \cup_i C_V(H_i)$ the pair x, y is a base of size 2. To complete this argument we need the following lemma.

Lemma 4.3. *Let us choose $x \in V$ such that $C_G(x)$ is isomorphic to the minimal stabilizer. If one of the following holds, then there exists $y \in V$ such that $C_G(x) \cap C_G(y) = 1$.*

(1) *$C_G(x)$ has less than $p+1$ minimal subgroups.*
(2) *More generally, $C_G(x)$ has $r+t$ minimal subgroups $H_1, \dots, H_{r+t}$ with $\dim C_V(H_i) \leq n-2$ for $r+1 \leq i \leq r+t$ and with $rp - r + t + 1 < p^2$.*

Proof. (1) Let $H_1, H_2, \dots, H_r$ be the minimal subgroups of $C_G(x)$ where $r < p+1$. Since the vector space V over the field of p elements cannot be covered by fewer than $p+1$ proper subspaces, we have $\cup_i C_V(H_i) \neq V$ so $C_G(x) \cap C_G(y) = 1$ holds for any $y \in V \setminus \cup_i C_V(H_i)$.

(2) Using the assumptions we have

$$\left|\cup_{i=1}^{r+t} C_V(H_i)\right| \leq rp^{n-1} - (r-1)p^{n-2} + tp^{n-2} = p^{n-2}(rp - r + t + 1) < p^n.$$

Therefore, $\cup_{i=1}^{r+t} C_V(H_i) \neq V$ and $C_G(x) \cap C_G(y) = 1$ holds for any element $y \in V \setminus \cup_i C_V(H_i)$.

□

Now, we can prove the following

Theorem 4.4. *Suppose p is a prime, V is an n-dimensional vector space over $\mathbb{F}_p$ and $G \leq GL(V)$ is a p'-group having a quasisimple normal subgroup N which is irreducible on V. Then there exist $x, y \in V$ such that $C_G(x) \cap C_G(y) = 1$.*

Proof. We only have to deal with the cases where there is no regular orbit. By using Theorem 4.1, first assume that $N = \mathrm{Alt}(c)$, the alternating group of degree c for $c < p$ acting on the deleted permutation module V for N. Let W be the natural permutation module for $N = \mathrm{Alt}(c)$ over $\mathbb{F}_p$. Then $W = V \oplus U$, where

$$V = \left\{(a_1, \dots, a_c) \in W \,\middle|\, \sum_i a_i = 0\right\} \text{ and } U = \left\{(a, \dots, a) \,\middle|\, a \in \mathbb{F}_p\right\}$$

are the deleted permutation module and the the trivial module for N, respectively.

Let $e_1, e_2, \dots, e_c \in W$ be a basis of W permuted by N in the usual way and let $x \in V$ be the image of the vector $e_1 + 2e_2 + 3e_3 + \dots + ce_c$ by the projection onto V along U. Obviously, $C_G(x) \cap N = 1$. Let $K = C_G(x) \cap NZ(G)$. Then $C_G(x)/K$ is isomorphic to a subgroup of $G/NZ(G)$. We claim that $|G : NZ(G)| \leq 2$. As V is an absolutely irreducible $\mathbb{F}_pN$-module, it follows that $C_G(N) = Z(G)$, hence $G/NZ(G)$ is embedded in $\mathrm{Out}(N)$. This group is isomorphic to C_2, unless $c = 6$. For $c = 6$ our claim follows from the observation that for any $g \in G \leq GL(V)$ the conjugation by g on N preserves the trace, so it fixes both conjugacy classes of elements of $N \simeq \mathrm{Alt}(6)$ of order 3 (since they have trace 2 and -1, respectively). However, every automorphism in $\mathrm{Aut}(\mathrm{Alt}(6)) \setminus \mathrm{Sym}(6)$ moves one of these classes to the other, so $G/NZ(G)$ is embedded into $\mathrm{Sym}(6)/\mathrm{Alt}(6) \simeq C_2$, as claimed. Thus, $C_G(x)/K \leq C_2$ holds for any c.

On the other hand, using that $K \cap N = 1$, it follows that K is isomorphic to a subgroup of $Z(G) \leq \mathbb{F}_p^\times$ and $C_G(x)$ acts trivially on K. Hence $C_G(x) \geq K \geq 1$ is a central chain of $C_G(x)$ and $C_G(x)$ is Abelian. As any coprime Abelian linear group has a regular orbit, we get G has a base of size two.

Now, we investigate the groups listed in part (2) of Theorem 4.1. Let us choose $x \in V$ such that $C_G(x)$ is isomorphic to the minimal stabilizer that can be seen

in Table 2. Using part (1) of Lemma 4.3 we can prove the existence of a suitable $y \in V$ unless G, n and p are one of the following

	G	n	p	minimal stabilizer
1	$U_4(2) \times Z$	5	7	S_4
2	$U_4(2).2 \times Z$	6	7	D_{12}
3	$2.U_4(2) \star Z$	4	7	U_{72}
4	$6_1.U_4(3).2_2 \star Z$	6	13	$W(B_3)$
5	$2.\Omega_8^+(2) \star Z$	8	11	$W(B_3)$

We deal with these cases one by one. If $C_G(x)$ is isomorphic to S_4, $W(B_3)$ or D_{12}, then we can use the complex character table of the group in order to find the dimension of the subspace $C_V(H) \leq V$ for a minimal subgroup $H \leq C_G(x)$. Indeed, in these cases every entry of the (complex) character table of $C_G(x)$ is a rational integer, so $C_G(x)$ has the same set of irreducible characters over $\mathbb{F}_p$ as it has over $\mathbb{C}$ by using [19, Theorem 15.13] and [19, Theorem 9.14].

Case 1 ($\mathbf{C_G(x) \simeq S_4}$): First, let us assume that $C_G(x) \simeq S_4$ and $(n, p) = (5, 7)$, so V can be viewed as a faithful $\mathbb{F}_7 S_4$-module. Now, for $\psi \in \mathrm{Irr}(S_4)$ we have $A_4' \leq \ker \psi$ if and only if $\psi(1) \neq 3$. It follows that V contains a faithful irreducible $\mathbb{F}_7 S_4$-submodule U of dimension 3. Now, the character of S_4 corresponding to U is one of the following:

	(1)	(12)	(12)(34)	(123)	(1234)
ψ_1	3	1	-1	0	-1
ψ_2	3	-1	-1	0	1

Let X_1 and X_2 be the matrix representations of S_4 over $\overline{\mathbb{F}_7}$ with characters ψ_1 and ψ_2, respectively. It follows easily from the character values and the order of the elements that

$$X_1((12)) \sim \mathrm{diag}(1, 1, -1), \quad X_2((12)) \sim \mathrm{diag}(1, -1, -1),$$
$$X_1((12)(34)) \sim X_2((12)(34)) \sim \mathrm{diag}(1, -1, -1),$$
$$X_1((123)) \sim X_2((123)) \sim \mathrm{diag}(1, \varepsilon, \varepsilon^2).$$

Here $\varepsilon \in \overline{\mathbb{F}_7}$ is a primitive 3rd root of unity and $\sim$ denotes conjugacy in the group $GL_3(\overline{\mathbb{F}_7})$. If H is a minimal subgroup of S_4, then $H = \langle h \rangle$ for some $h \in S_4$ of order 2 or 3. It follows from the above matrix forms that for an element $h \in C_G(x)$ of order 2 or 3 we have $\dim C_U(h) \leq 1$ for $h \in A_4$ and $\dim C_U(h) \leq 2$ for $h \in S_4 \setminus A_4$. Using part (2) of Lemma 4.3 with $r = 6$, $t = 7$ and $p = 7$ we can choose $y \in U \leq V$ such that $C_G(x) \cap C_G(y) = 1$ holds.

Case 4 and 5 ($\mathbf{C_G(x) \simeq W(B_3)}$): Now, $C_G(x) \simeq W(B_3) \simeq S_4 \times K$ for $K = \langle k \rangle \simeq C_2$, so every $\chi \in \mathrm{Irr}(W(B_3))$ is of the form $\chi = \psi \times \lambda$ for some $\psi \in \mathrm{Irr}(S_4)$ and $\lambda \in \mathrm{Irr}(K)$. Again, $W(B_3)$ acts faithfully on V, so, by using the same argument as in Case 1, V contains an irreducible $\mathbb{F}_p W(B_3)$-submodule U of dimension 3 and $S_4 \leq W(B_3)$ acts faithfully on U. If K acts trivially on U, then, by Case 1, we can find $y_1 \in U$ such that $C_G(x) \cap C_G(y_1) = K$. Let $V = U \oplus U_2$ for some $\mathbb{F}_p C_G(x)$-submodule U_2. As K acts faithfully on U_2, there is a $y_2 \in U_2$ such that $C_K(y_2) = 1$. By choosing $y = y_1 + y_2$ we get $C_G(x) \cap C_G(y) = 1$. If K acts faithfully on U, let $\chi = \psi \times \lambda$ be the character corresponding to U. Then $\psi \in \mathrm{Irr}(S_4)$, $\psi(1) = 3$

and $\lambda(k) = -1$ holds. By Case 1, either $\psi = \psi_1$ or $\psi = \psi_2$. In either case, $U = C_U(g) \oplus C_U(gk)$ for any $g \in S_4$ with $o(g) = 2$. Therefore,

$$|\{H \leq C_G(x) \,|\, |H| = 2,\, \dim C_U(H) = 1\}| \\ = |\{H \leq C_G(x) \,|\, |H| = 2,\, \dim C_U(H) = 2\}| = 9.$$

Now, we can apply part 2 of Lemma 4.3 with $r = 9,\ t = 14$ and $p \geq 11$ to get a $y \in U$ such that $C_G(x) \cap C_G(y) = 1$.

Case 2 ($\mathbf{C_G(x) \simeq D_{12}}$): In this case we have $C_G(x) \simeq D_{12} = \langle f, t \,|\, f^6 = t^2 = 1,\ tft = f^{-1} \rangle$. Now, $D'_{12} = \langle f^2 \rangle$ and D_{12} has four linear characters and 2 irreducible characters of degree two. As D_{12} acts faithfully on V it follows that V contains an irreducible $\mathbb{F}_p D_{12}$-submodule U of dimension 2. Now, the character corresponding to U is one of the following

	1	f^3	$\{f, f^5\}$	$\{f^2, f^4\}$	$\{t, f^2t, f^4t\}$	$\{ft, f^3t, f^5t\}$
ψ_1	2	2	-1	-1	0	0
ψ_2	2	-2	1	-1	0	0

If the character related to U is ψ_1, then $D_{12}/\ker(\psi_1) \simeq D_6$ acts faithfully on U, so, by using part (1) of Lemma 4.3 we can find a $y_1 \in U$ such that $C_G(x) \cap C_G(y_1) = \langle f^3 \rangle$. Let $V = U \oplus U_2$ for some $\mathbb{F}_p C_G(x)$-submodule U_2. Now, $\langle f^3 \rangle$ acts faithfully on U_2, so $C_{\langle f^3 \rangle}(y_2) = 1$ for some $y_2 \in U_2$. By choosing $y = y_1 + y_2$ we get $C_G(x) \cap C_G(y) = 1$. If the character related to U is ψ_2, then D_{12} acts faithfully on U. Now, D_{12} has seven subgroups of order 2 and only one of order 3, the one generated by f^2. However, in this case the related matrix $X_2(f^2) \simeq \mathrm{diag}(\varepsilon, \varepsilon^2)$ for some $\varepsilon \in \overline{\mathbb{F}_p}$, where ε is a primitive 3rd root of unity, so f^2 does not fix any vector in $U \setminus \{0\}$. Applying part (2) of Lemma 4.3 with $r = 7,\ t = 1$ and $p = 7$ we get a $y \in U$ such that $C_G(x) \cap C_G(y) = 1$.

Case 3 ($\mathbf{C_G(x) = U_{72}}$): Although one can show that also in this case there is a regular orbit on V for $C_G(x)$, we present here a simpler proof due to P. P. Pálfy by showing that there is a two-dimensional subspace of $V \simeq \mathbb{F}_7^4$ with trivial pointwise stabilizer in $G = 2.U_4(2) \star \mathbb{F}_7^\times \simeq 2.U_4(2) \times C_3$. Let $N = 2.U_4(2)$ and $a \in G$ a central element of order 3, so $G = N \times \langle a \rangle$. For each prime divisor $p \mid |G|$, i.e. for $p = 2, 3, 5$, let

$$n_p := |\{U \leq V \mid \dim U = 2,\ \exists g \in G : o(g) = p \text{ and } U \leq C_V(g)\}|.$$

By using the character table of $N = 2.U_4(2)$ found in the Atlas [8, page 27], one sees that the corresponding Brauer character of the $\mathbb{F}_7 G$-module V is one of the two conjugate characters $\chi_{21}, \chi_{22} \in \mathrm{Irr}(N)$. Since we are only interested in dimensions of fixed point spaces of elements of G, we can assume that the Brauer character of V is χ_{21}.

Now, for each prime divisor $p \mid |G|$ and for each conjugacy class $\mathcal{C} \subseteq N$ consisting of elements of order p, the following table contains the size of $\mathcal{C}$, the character value of χ_{21} on $\mathcal{C}$, and its unique decomposition as a sum of four p-th roots of unity. Here ε and ω denote a primitive third and fifth root of unity, respectively. Furthermore, we use the Atlas notation for conjugacy classes.

p	conj. class $\mathcal{C}$	$\lvert\mathcal{C}\rvert$	$\chi_{21}(g)$ $(g \in \mathcal{C})$	decomposition
2	2A	1	-4	-1-1-1-1
	2B	90	0	-1-1+1+1
3	3A	40	$-1/2 + 3\sqrt{3}/2i$	$1+1+1+\varepsilon$
	3B	40	$-1/2 - 3\sqrt{3}/2i$	$1+1+1+\varepsilon^2$
	3C	240	-2	$\varepsilon+\varepsilon+\varepsilon^2+\varepsilon^2$
	3D	480	1	$1+1+\varepsilon+\varepsilon^2$
5	5A	5184	-1	$\omega+\omega^2+\omega^3+\omega^4$

It follows that $n_2 \leq 90$ and $n_5 = 0$. Furthermore, if $(n, a^k) \in N \times \langle a \rangle$ is an element of order 3, then

$$\dim C_V((n,a^k)) = \begin{cases} 3 & \text{if } n \in 3A \cup 3B,\ a^k = 1, \\ 2 & \text{if } n \in 3C,\ a^k \neq 1, \\ 2 & \text{if } n \in 3D,\ a^k = 1, \\ \leq 1 & \text{otherwise.} \end{cases}$$

As the number of two-dimensional subspaces in a three dimensional subspace of V is 57 we get

$$\begin{aligned} &|\{(U,g) \,|\, U \leq V,\ \dim U = 2,\ g \in G,\ o(g) = 3,\ U \leq C_V(g)\}| \\ &\qquad \leq 2 \cdot 40 \cdot 57 + 240 \cdot 2 + 480 = 5520. \end{aligned}$$

Since $C_V(g) = C_V(g^{-1})$ for any $g \in G$ and the intersection of two three dimensional subspaces in V is a two dimensional subspace, we get $n_3 < 5520/2 = 2760$.

Hence the number of two dimensional subspaces of V fixed pointwise by some minimal subgroup of G is less than $90 + 2760 = 2850$. However, the total number of two dimensional subspaces of V is exactly 2850, which completes our proof. □

Remark 4.5. We note that for all the cases in the table on page 13, one can easily find a two element base by using an appropriate computer algebra system (e.g. GAP or Magma), so our ad hoc approach using character theory is not really necessary to handle these cases.

5. Groups of symplectic type

The purpose of this section is to prove Theorem 1.1 for coprime linear groups of symplectic type, thus we handle the case (c) given at the end of Section 2. First we collect a number of facts about the structure and representations of extraspecial r-groups in Section 5.1, starting with the definition of the concept of groups of symplectic type.

In this section V is an $n > 1$ dimensional vector space over the field $\mathbb{F}_q$ of characteristic p and $G \leq GL(V)$ is a coprime linear group with normal subgroups $Z \leq N \leq G$ such that $Z \simeq \mathbb{F}_q^\times$ is the group of scalar transformations and N/Z is a minimal normal subgroup of G/Z.

5.1. The structure and action of N.

Definition 5.1. Using the above notation, we say that G is of symplectic type if the quotient group $N/Z \lhd G/Z$ is an elementary abelian r-subgroup for some prime number r, and V is an absolutely irreducible $\mathbb{F}_qN$-module.

Remark 5.2. Note that with these assumptions, $r \neq p$ holds. This follows immediately since G is coprime, but it is true even if we drop the coprime assumption for G. As we will see shortly, r must divide $q-1$.

Recall that for a prime number r, an r-group E is called an extraspecial r-group if $E' = Z(E) \simeq C_r$. If R is any r-group, then $\Omega_1(R)$ denotes the subgroup of R generated by all the elements of order r.

Lemma 5.3. *We have $N = E \star Z$, where E is an extraspecial r-group, $E' = Z(E) = E \cap Z \simeq C_r$ and V is a faithful and absolutely irreducible $\mathbb{F}_q E$-module.*

Proof. As any absolutely irreducible representation of an Abelian group is one-dimensional, N cannot be Abelian. Let R be the Sylow-r subgroup of N. Then $N = RZ$, so $N' = R'$. Furthermore, $Z(R) = R \cap Z$.

The group $R/Z(R) \simeq N/Z$ is Abelian, so $[x,y]^r = [x^r, y] = 1$ holds for every $x, y \in R$ by [1, 8.6 (1)]. As Z is a cyclic group of order $q-1$, we see that r divides $q-1$ and R' coincides with the unique subgroup of Z of order r. The quotient group R/R' is Abelian, but non-cyclic. Indeed, otherwise N/Z would also be cyclic, so N would be Abelian, a contradiction.

Let $L \geq R'$ be the full inverse image of the subgroup $\Omega_1(R/R')$, so L is a characteristic subgroup of R. In particular, $L \lhd G$. As R/R' is non-cyclic, L/R' is a vector space over $\mathbb{F}_r$ of dimension bigger than one, so L is not contained in Z. Therefore, $Z < LZ \leq N$ and $LZ \lhd G$. Since N/Z is a minimal normal subgroup of G/Z we get $LZ = N$.

If $L \cap Z = R'$, then L is extraspecial, so $E = L$ is a good choice. Finally, if $L \cap Z > R'$, then $(L \cap Z)/R'$ is a one dimensional subspace in L/R'. Then we can choose E as a full inverse image of a direct complement of $(L \cap Z)/R'$ in L/R'. □

In the next theorem we collect some of the basic properties of the extraspecial r-group E in Lemma 5.3.

Theorem 5.4. *With an appropriate choice of E, one can guarantee that the following properties hold:*

1. *For $r > 2$, E is of exponent r. Then E is a central product of k copies of the unique non-Abelian r-group of order r^3 and of exponent r.*
2. *For $r = 2$, there are two possibilities:*
   (a) *E is a central product of k copies of the dihedral group D_8 of order eight.*
   (b) *E is a central product of $k-1$ copies of the dihedral group D_8 and one quaternion group Q_8.*
3. *E is a product of two elementary Abelian r-groups of order r^{k+1}, unless $r = 2$, $q \equiv -1 \mod 4$ and (2)(b) holds.*
4. *With the above notation, $|E| = r^{2k+1}$ and $n = r^k$.*

Proof. First, let us assume that r is odd. Then $\Omega_1(R)$ has exponent r by [1, 23.11]. Now, $|\Omega_1(R)| > r$ by [18, 8.2 Satz a]. Therefore, $\Omega_1(R)$ is not a subgroup of Z, so $Z < \Omega_1(R)Z \leq N$. As $\Omega_1(R)$ is a characteristic subgroup of N, we also have $\Omega_1(R)Z \lhd G$. Using that N/Z is a minimal normal subgroup of G/Z, $\Omega_1(R)Z = N$ follows. By choosing $E = \Omega_1(R)$ we obtain an extraspecial r-group E of exponent r such that $N = E \star Z$. Thus, the first assertion of part (1) follows.

The second assertion of part (1) and part (2) are just the statements [1, 23.13] and [1, 23.14], respectively.

Now let us consider parts (3) and (4). Write $E = E_1 \star E_2 \star \ldots \star E_k$, a central product of k non-Abelian groups of order r^3. If each E_i is of exponent r (for $r > 2$) or each E_i is isomorphic to D_8 (for $r = 2$), then we can choose $x_i, y_i \in E_i$ of order r such that $E_i = \langle x_i, y_i \rangle$. Then $\langle x_1, \ldots, x_k, Z(E) \rangle$ and $\langle y_1, \ldots, y_k, Z(E) \rangle$ are two elementary Abelian groups of order r^{k+1} such that E is equal to their product. Finally, if R is a central product of $k-1$ dihedral groups D_8 and a quaternion group $Q_8 = \langle i, j \rangle \leq E$ and $q \equiv 1 \mod 4$, then let $\lambda \in Z$ be an element of order 4. By defining $H = \langle \lambda i, \lambda j \rangle \leq ZQ_8$ we get $H \simeq D_8$ and $ZH = ZQ_8$. So we can replace E by a central product of k dihedral groups and we can apply the previous argument to complete the proof of part (3).

Finally, part (4) follows immediately from the description of the irreducible representations of extraspecial r-groups over their splitting fields of characteristic different from r, which can be found e.g. in [1, 34.9]. □

Definition 5.5. We say that N is non-monomial, if $r = 2$, $q \equiv -1 \mod 4$, and E is a central product of some dihedral groups D_8 of order eight and one quaternion group Q_8. Otherwise, we say that N is monomial.

The explanation of our terminology is that N is monomial if and only if V is a monomial representation of N. We will see this in the following two theorems, which give us a more detailed description of the $\mathbb{F}_q N$-module V.

Theorem 5.6. *Using the above notation, let us assume that N is monomial. Then there is a decomposition $N = D \rtimes S$ and a suitable basis $\{u_1, u_2, \ldots, u_n\}$ of V with the following properties:*

1. *$D = Z \times D_1$ and $D_1 \simeq S \simeq C_r^k$ for $r^k = n$.*
2. *With respect to $u_1, u_2, \ldots, u_n$, the subgroup $S \leq GL(n, q)$ consists of permutation matrices. Moreover, S acts regularly on this basis.*
3. *With respect to $u_1, u_2, \ldots, u_n$, the subgroup $D \leq GL(n, q)$ consists of diagonal matrices. The subspaces $\langle u_i \rangle$, $1 \leq i \leq n$ are all the irreducible representations of D_1 with $\langle u_1 \rangle$ being the trivial representation of D_1, and they are pairwise non-equivalent. Moreover, the main diagonal of every $g \in D_1 \leq GL(n, q)$ contains all of the $o(g)$-th roots of unity with the same multiplicity.*

Proof. According to part (3) of Theorem 5.4, let $E = D_E S_E$ be a product of two elementary abelian groups of order r^{k+1}, $D = ZD_E$ and S a complement of $Z(E)$ in S_E. Then $N = D \rtimes S$. As $\mathbb{F}_q$ contains the $\exp(D)$-th roots of unity (recall that r divides $q-1$), every irreducible $\mathbb{F}_q D$-module is one-dimensional. Fix $u_1 \in V$ such that $\langle u_1 \rangle$ is a one dimensional D-invariant subspace. Choosing $D_1 = C_D(u_1)$ we have $D = Z \times D_1$ and $D_1 \simeq S \simeq C_r^k$. By part (4) of Theorem 5.4 we have $r^k = n$, hence part (1) holds.

Let $S = \{s_1, s_2, \ldots, s_n\}$ and for each $1 \leq i \leq n$ let u_i be defined as $u_i = s_i(u_1)$. Since $D \lhd N$, by Clifford theory we have $\langle u_i \rangle$ is a D-invariant subspace for each $1 \leq i \leq n$. Hence $\langle u_1, u_2, \ldots, u_n \rangle$ is a $DS = N$-invariant subspace, so it is equal to V. As $n = |S| = \dim V$, it follows that $u_1, u_2, \ldots, u_n$ is a basis of V and S acts regularly on this basis. So part (2) follows.

We have already seen in the last paragraph that $\langle u_i \rangle$ is a D-invariant subspace for each i, hence $D \leq GL(n, q)$ consists of diagonal matrices with respect to $u_1, u_2, \ldots, u_n$. The claim that $\langle u_i \rangle$ are pairwise non-equivalent $\mathbb{F}_q D_1$-modules

follows easily from the fact $C_S(D_1) = 1$. Indeed, let $u_i \neq u_j$ be two basis elements. Then $u_j = su_i$ for some $s \in S \setminus \{1\}$. Let $d \in D_1$ such that $[d, s] \in Z \setminus \{1\}$, and let $d = \mathrm{diag}(d_1, \ldots, d_n)$ be the diagonal form of d. Then $d_j u_j = [d, s](d_i u_j)$, so $d_j \neq d_i$ which proves that the $\langle u_i \rangle$ and $\langle u_j \rangle$ are non-isomorphic $\mathbb{F}_q D_1$-modules. As $|D_1| = n$, these are all the irreducible representations of D_1. Furthermore, $\langle u_1 \rangle$ is the trivial representation of D_1 by definition. Finally, if $g \in D_1$, then any linear representation of $\langle g \rangle$ can be extended to D_1 in exactly $|D_1|/o(g)$ ways, which completes the proof of part (3). □

Remark 5.7. In view of this theorem, every $n \in N$ is a monomial matrix with respect to the basis $\{u_1, u_2, \ldots, u_n\}$. Thus, every $n \in N$ has a unique decomposition $n = \delta(n)\pi(n)$ to a product of a diagonal matrix $\delta(n) \in D$ and a permutation matrix $\pi(n) \in S$.

We finish this section with a similar result in the case where N is non-monomial. Since we will also use Theorem 5.6 in this case, it is convenient to write U rather than V for the remainder of this discussion of the non-monomial case. Thus, U is an $n = 2^k$ dimensional vector space over $\mathbb{F}_q$, and it is absolutely irreducible as an $\mathbb{F}_q N$-module. Furthermore, $q \equiv -1 \mod 4$ and $N = Q_8 \star N_1$, where N_1 is a central product of $k - 1$ dihedral groups of order 8 and the group of scalar matrices. Using [26, Corollary 18.2(a)] it follows that $U = W \otimes V$, for some faithful absolutely irreducible $\mathbb{F}_q Q_8$-module W and for some faithful absolutely irreducible $\mathbb{F}_q N_1$-module V. Since Q_8 has a unique faithful irreducible representation over $\mathbb{F}_q$, and it is 2-dimensional, we have $\dim W = 2$ and $\dim V = n/2$. Let $\{w_1, w_2\}$ be a basis of W and $V_1 = \langle w_1 \rangle \otimes V$, $V_2 = \langle w_2 \rangle \otimes V$. Then $U = V_1 \oplus V_2$ is a direct sum decomposition of U into irreducible $\mathbb{F}_q N_1$-modules. Let $N_G(V_1)$ be the elements of G that fix V_1 setwise. The restriction of $N_G(V_1)$ to $V_1 \simeq V$ defines a homomorphism $N_G(V_1) \to GL(V)$ with image $G_1 \simeq N_G(V_1)/C_G(V_1)$. Furthermore, the restriction of $N_1 \leq N_G(V_1)$ to V_1 defines a subgroup of G_1 isomorphic to N_1. Thus, $N_1 \leq G_1 \leq GL(V)$ and we have the monomial case situation. We will now use Theorem 5.6 to prove the following result:

Theorem 5.8. *In terms of the above notation, the following holds*

(1) *There is a decomposition $N_1 = D \rtimes S$, such that $D = Z \times D_1$ and $D_1 \simeq S \simeq C_2^{k-1}$. Furthermore, $N = (Q_8 \star D) \rtimes S$.*
(2) *There is a basis $\{u_1, u_2, \ldots, u_{n/2}\}$ of V with the following properties*
   (a) *For each $1 \leq i \leq n/2$ let $W_i = W \otimes \langle u_i \rangle$. Then $W_1, W_2, \ldots, W_{n/2}$ are exactly the homogeneous components of $Q_8 D$ (or D or D_1). The elements of D act as scalar matrices on each W_i. Furthermore, $D_1 = C_N(W_1)$.*
   (b) *S acts regularly on the sets $\{w_1 \otimes u_1, w_1 \otimes u_2, \ldots, w_1 \otimes u_{n/2}\}$ and $\{w_2 \otimes u_1, w_2 \otimes u_2, \ldots, w_2 \otimes u_{n/2}\}$. Thus, S permutes the subspaces $W_1, \ldots, W_{n/2}$ regularly.*
   (c) *For any $n \in N$ there is a unique decomposition $n = \delta(n)\pi(n)$ with $\delta(n) \in Q_8 D$ and $\pi(n) \in S$. Furthermore, n is a monomial matrix if and only if $\delta(n) \in D$.*
(3) *If $g \in Q_8 D$ has an eigenvector in U, then $g \in D$.*

Proof. The decomposition of N_1 in part (1) of the theorem follows if one applies part (1) of Theorem 5.6 to N_1.

For part (2), we define the basis $\{u_1, u_2, \ldots, u_{n/2}\}$ of V as it was defined in Theorem 5.6. In view of the definition of tensor product of modules, we see that each W_i is isomorphic to W as an $\mathbb{F}_q Q_8$-module, while it is isomorphic to $\langle u_i\rangle \oplus \langle u_i\rangle$ as an $\mathbb{F}_q D$-module. As $\langle u_1\rangle, \ldots, \langle u_{n/2}\rangle$ are all the irreducible representations of D, which are pairwise non-equivalent (see part (3) of Theorem 5.6), part (2)(a) follows. As S permutes the basis vectors $\{u_1, u_2, \ldots, u_{n/2}\}$ regularly by part (2) of Theorem 5.6 it also permutes the subspaces $W_1, \ldots, W_{n/2}$ regularly, so part (2)(b) holds. Now, part (2)(c) is a trivial consequence of the last two statements.

To prove (3), first notice that if $g \in Q_8 D$ but $g \notin D$, then $o(g)$ is divisible by 4. This follows from the facts that Q_8 commutes with D, every element from $Q_8 \setminus Q_8 \cap D$ has order four, but no elements of D has order divisible by four (recall that $q \equiv -1 \pmod 4$). Thus, $g^{o(g)/2}$ must be an element of Q_8 of order 2, so it must be $-I$. Therefore, if $\lambda \in \mathbb{F}_q$ is an eigenvalue of g, then $\lambda^{o(g)/4} \in \mathbb{F}_q$ is a primitive fourth root of unity, a contradiction. □

Remark 5.9. In contrast to the monomial case, $\delta(n)$ is not necessarily a monomial matrix, but a block diagonal matrix containing 2×2 blocks.

5.2. **Finding a two-element base when N is monomial.** In this section we find a two element base for G when N is monomial. As in Theorem 5.6, fix an $\mathbb{F}_q$-basis $\{u_1, u_2, \ldots, u_n\}$ for V and write $N = D \rtimes S$ and $D = Z \times D_1$, where $D_1 = C_D(u_1) \simeq S \simeq C_r^k$. Note that $D_1 = C_N(u_1)$.

Theorem 5.10. *Let $g \in G_G(u_1)$. Then*

(1) *$D_1^g = D_1$ and g is a monomial matrix. Hence there exists a unique decomposition $g = \delta(g)\pi(g)$ as a product of a diagonal matrix $\delta(g)$ and a permutation matrix $\pi(g)$.*
(2) *$\pi(g)$ normalizes S, that is, $S^{\pi(g)} = S$.*
(3) *Both $\delta(g)$ and $\pi(g)$ normalize N, so $N = N^{\delta(g)} = N^{\pi(g)}$. Moreover, $[\delta(g), S] \subseteq D$.*
(4) *If $\delta(g) \neq 1$, then the number of 1's in the main diagonal of $\delta(g)$ is at most $\frac{3}{4}n$.*

Proof. The statement $D_1^g = D_1$ follows from the fact $D_1 = C_N(u_1) \lhd C_G(u_1)$. Consequently, g permutes the homogeneous components of the D_1-module V. By part (3) of Theorem 5.6, these homogeneous components are just the one-dimensional subspaces $\langle u_i\rangle$ for $1 \leq i \leq n$. It follows that g is a monomial matrix. Of course, a monomial matrix g has a unique decomposition $g = \delta(g)\pi(g)$, and part (1) is proved.

With respect to the basis $\{u_1, u_2, \ldots, u_n\}$, let M and P denote the group of monomial matrices and the group of permutation matrices, respectively. Thus, $N \leq M$ and $g \in M$. Let $\pi : M \to P$ be the homomorphism which maps each monomial matrix into its permutation part. As $g \in G$ normalizes N, it follows that $\pi(g)$ normalizes $\pi(N) = S$ and (2) follows.

Both g and $\delta(g)$ normalize D, hence $\pi(g) = \delta(g)^{-1}g$ also normalizes D. We have already seen that $\pi(g)$ normalizes S, so it also normalizes $N = DS$. Therefore $\delta(g) = g\pi(g)^{-1}$ also normalizes N. Finally, $[\delta(g), S]$ is a subset of N and it consists of diagonal matrices, so $[\delta(g), S] \subseteq D$ and (3) holds.

If $\delta(g) \neq 1$, then $\delta(g)$ is not a scalar matrix, so there exists an $s \in S$ such that $[\delta(g), s] \in D \setminus \{1\}$. Using part (3) of Theorem 5.6, we get that the number of 1's

in the main diagonal of $[\delta(g), s]$ is at most $\frac{1}{2}n$. This cannot be true if the number of 1's in $\delta(g)$ is more than $\frac{3}{4}n$. We are done. □

By part (2) of Theorem 5.6, S acts regularly on the basis $W = \{u_1, \dots, u_n\}$. Identifying u_1 with the identity element of S, this action defines a vector space structure on W isomorphic to $\mathbb{F}_r^k$. Viewing W in this way as an $\mathbb{F}_r$-vector space, the zero element of W is u_1. (Here it may be a bit confusing that W is a basis of the original space, while it itself has a vector space structure inherited from the regular action of S on W).

Using the previous theorem, $C_G(u_1)$ consists of monomial matrices and its permutation part $\pi(C_G(u_1))$ acts by conjugation on S. In fact, this action is faithful, since $C_{GL(n,q)}(u_1) \cap C_{GL(n,q)}(S) = 1$. It follows that the action of $\pi(C_G(u_1))$ on W is linear, when we consider W as a vector space, so $\pi(C_G(u_1)) \leq GL(W) \simeq GL(k, r)$. Choosing a basis $\{e_1, e_2, \dots, e_k\} \subseteq W$, the next theorem helps us to find a "good" $\pi(C_G(u_1))$-regular partition of W.

Theorem 5.11. *Let $H \leq GL(W)$, where r is a prime and $W \simeq \mathbb{F}_r^k$ is an $\mathbb{F}_r$-space with basis $e_1, e_2, \dots, e_k$. Then there is an H-regular partition $W = \cup_i \Omega_i$ of W with the following properties*

1. *For $r \geq 3,\ k = 1$ we have $W = \{e_1\} \cup \Omega_2$ with $|\Omega_1| < \frac{1}{4}|W|$ if $|W| \neq 3$.*
2. *For $r \geq 3,\ k \geq 2$ we have $W = \{e_1\} \cup \Omega_2 \cup \Omega_3$ such that $|\Omega_2| + 2 < \frac{1}{4}|W|$ if $|W| \neq 9$.*
3. *For $r = 2,\ k \geq 3$ we have $|W| = \{e_1\} \cup \{e_2\} \cup \Omega_3 \cup \Omega_4$ such that $|\Omega_3| < \frac{1}{4}|W|$ if $|W| \neq 16$.*

Proof. First, let us assume that $r \geq 3$ and $k = 1$. Then

$$\Omega_1 = \{e_1\}, \quad \Omega_2 = W \setminus \Omega_1 \tag{P.1}$$

is an H-regular partition of the one dimensional space W with $|\Omega_1| = 1 < \frac{5}{4} \leq \frac{1}{4}|W|$ if $r \geq 5$.

In case of $r \geq 3,\ k \geq 2$ let

$$\Omega_1 = \{e_1\}, \quad \Omega_2 = \{e_2, e_3, \dots, e_k, e_1 + e_2, e_2 + e_3, \dots, e_{k-1} + e_k\}, \quad \Omega_3 = W \setminus (\Omega_1 \cup \Omega_2). \tag{P.2}$$

To prove that this is an H-regular partition of W, let $h \in H$ be an element fixing setwise both Ω_1 and Ω_2. By using induction on t, we prove that $he_t = e_t$ for each $1 \leq t \leq k$, that is, $h = 1$. First, our choice $\Omega_1 = \{e_1\}$ guarantees that $he_1 = e_1$. Assuming that $he_i = e_i$ for all $1 \leq i < t \leq k$, it follows that $h(e_t)$ and $h(e_{t-1} + e_t)$ are elements of the set

$$\Omega_2 \setminus \langle e_1, \dots, e_{t-1} \rangle = \{e_t, e_{t+1}, \dots, e_k, e_{t-1} + e_t, \dots, e_{k-1} + e_k\}.$$

Since $h(e_{t-1} + e_t) - h(e_t) = e_{t-1}$, it follows that either $h(e_t)$ or $h(e_{t-1} + e_t)$ contains e_{t-1} with non-zero coefficient. However, there is only one element in $\Omega_2 \setminus \langle e_1, \dots, e_{t-1} \rangle$ with this property, namely, $e_{t-1} + e_t$. So either $h(e_{t-1} + e_t) = e_{t-1} + e_t$ or $h(e_t) = e_{t-1} + e_t$. In the latter case $h(e_{t-1} + e_t) = 2e_{t-1} + e_t \notin \Omega_2$, since $r \neq 2$, a contradiction. It follows that $h(e_{t-1} + e_t) = e_{t-1} + e_t$, so $h(e_t) = h(e_{t-1} + e_t) - h(e_{t-1}) = e_t$. Thus, $he_t = e_t$ for each $1 \leq t \leq k$, which proves that the given partition is H-regular. The inequality $|\Omega_2| + 2 = 2k < \frac{1}{4}r^k = \frac{1}{4}|W|$ holds for $k \geq 2,\ r \geq 5$ or for $k \geq 3,\ r = 3$, but it fails for $k = 2,\ r = 3$, which proves (2).

For $r = 2,\ k = 3$ let

$$\Omega_1 = \{e_1\}, \quad \Omega_2 = \{e_2\}, \quad \Omega_3 = \{e_3\}, \tag{P.3}$$
$$\Omega_4 = W \setminus (\Omega_1 \cup \Omega_2 \cup \Omega_3) = \{0, e_1 + e_2, e_1 + e_3, e_2 + e_3, e_1 + e_2 + e_3\},$$

while for $r = 2,\ k \geq 4$ let

$$\Omega_1 = \{e_1\}, \quad \Omega_2 = \{e_2\},$$
$$\Omega_3 = \{e_3, \ldots, e_k, e_2 + e_3, e_3 + e_4, e_4 + e_5, \ldots, e_{k-1} + e_k, e_k + e_1\}, \tag{P.4}$$
$$\Omega_4 = W \setminus (\Omega_1 \cup \Omega_2 \cup \Omega_3).$$

Now, for $k = 3$, the above partition is clearly H-regular, since we fixed each element of the basis e_1, e_2, e_3. Furthermore, $|\Omega_3| = 1 < 2 = \frac{1}{4}|W|$ holds. In case $k \geq 4$, we prove that the given partition is H-regular by using a similar argument as we did in case (2). Let $h \in H$ be an element fixing every element of the partition. Assuming that $h(e_i) = e_i$ for all $1 \leq i < t < k$ we get that $h(e_t)$ and $h(e_{t-1} + e_t)$ are elements of the set

$$\Omega_3 \setminus \langle e_1, \ldots, e_{t-1} \rangle = \{e_t, e_{t+1}, \ldots, e_k, e_{t-1} + e_t, \ldots, e_{k-1} + e_k, e_k + e_1\}.$$

Since $h(e_t) + h(e_{t-1} + e_t) = e_{t-1}$, we have either $h(e_{t-1} + e_t) = e_{t-1} + e_t$ or $h(e_t) = e_{t-1} + e_t$. In the former case we get $h(e_t) = e_t$, while in the latter case we can take $e_t + e_{t+1} \in \Omega_3$ since $t < k$. Now e_{t-1} occurs with 0 coefficient both in $h(e_t + e_{t+1})$ and $h(e_{t+1})$, since the only element of $\Omega_3 \setminus \langle e_1, \ldots, e_{t-1} \rangle$ containing e_{t-1} with nonzero coefficient is $h(e_t)$. However, $h(e_t + e_{t+1}) + h(e_{t+1}) = h(e_t) = e_{t-1} + e_t$, a contradiction. It remains to prove that $h(e_k) = e_k$. It is clear that

$$h(e_k) \in \Omega_3 \setminus \langle e_1, e_2, \ldots, e_{k-1} \rangle = \{e_k, e_{k-1} + e_k, e_k + e_1\}.$$

If $h(e_k) = e_{k-1} + e_k$, then $h(e_k + e_1) = e_{k-1} + e_k + e_1 \notin \Omega_3$. If $h(e_k) = e_k + e_1$, then $h(e_{k-1} + e_k) = e_{k-1} + e_k + e_1 \notin \Omega_3$. Thus $h(e_k) = e_k$ also holds. It follows that $h = 1$, so the given partition is H-regular. Finally, $|\Omega_3| = 2k - 3 < 2^{k-2} = \frac{1}{4}|W|$ if $|W| > 16$. □

Theorem 5.12. *With the above notation, let us assume that $r \geq 3$ and set $x = u_1$. Furthermore, let $\alpha \in \mathbb{F}_q$ be a generator of the multiplicative group of $\mathbb{F}_q$. By using the displayed regular partitions (P.1) and (P.2) in the proof of Theorem 5.11 let y be defined as follows*

$$y = \begin{cases} \displaystyle\sum_{u_i \in \Omega_2} u_i & \text{if } k = 1 \text{ and } r > 3 \\ \alpha e_1 + \displaystyle\sum_{u_i \in \Omega_3} u_i & \text{if } k \geq 2 \text{ and } (k, r) \neq (2, 3) \\ y = \alpha e_1 + 0 \cdot e_2 + \displaystyle\sum_{u_i \notin \{e_1, e_2\}} u_i & \text{if } (k, r) = (2, 3) \\ y = \alpha u_2 + u_3 & \text{if } (k, r) = (1, 3). \end{cases}$$

Then $C_G(x) \cap C_G(y) = 1$.

Proof. Let $g \in C_G(x) \cap C_G(y)$. Since $g \in G$ fixes $x = u_1$, we get that g is a monomial matrix by part (1) of Theorem 5.10, thus we have a decomposition $g = \delta(g)\pi(g)$ with respect to the $\mathbb{F}_q$-basis $\{u_1, u_2, \ldots, u_n\}$ for V. Since g fixes y, note that $\pi(g)$ permutes the $u_i \in W$ that appear in y with a zero coefficient.

First assume that $k = 1$ and $r > 3$. Define Ω_1 and Ω_2 as in (P.1). Note that $\pi(g)$ fixes Ω_1. As $W = \Omega_1 \cup \Omega_2$ is a $\pi(C_G(u_1))$-regular partition, we get $\pi(g) = 1$.

Hence $g = \delta(g)$ is a diagonal matrix. If g_i denotes the i-th element of the main diagonal of g, then $g \in C_G(y)$ only if $g_i = 1$ for all $u_i \in \Omega_2$. As $|\Omega_2| > \frac{3}{4}|W|$, by using part (4) of Theorem 5.10, we get $g = \delta(g) = 1$.

Next assume that $k \geq 2$ and $(k, r) \neq (2, 3)$. Defin Ω_1, Ω_2 and Ω_3 as in (P.2). Observe that $\pi(g)$ fixes the subset $\Omega_2 \subseteq W$, since only the elements of Ω_2 occur with coefficient 0 in y. However, in this case it is possible that $\pi(g)$ moves the unique element of Ω_1 to an element of Ω_3. Of course, in that case it moves an element of Ω_3 to the element of Ω_1. This results in the appearance of an α and an α^{-1} in the main diagonal of $\delta(g)$. It follows that in the main diagonal of $\delta(g)$ the number of elements different from 1 is at most $|\Omega_2| + 2$, which is less than $\frac{1}{4}|W|$ by Theorem 5.11. Using part (4) of Theorem 5.10 we get $\delta(g) = 1$, hence $\pi(g)$ also fixes the unique element of Ω_1, so $g = \pi(g) = 1$.

Now assume $|W| = 9$, so $(k, r) = (2, 3)$ and the matrix $\pi(g)$ fixes e_2. If $\pi(g)$ does not fix e_1, then in the main diagonal of $\delta(g)$ there is an α and an α^{-1} and at most one more element not equal to 1. Since S acts regularly on W, we can choose an element $s \in S$ which takes the basis element corresponding to α^{-1} to the basis element corresponding to α. Then, the main diagonal of $[\delta(g), s] \in D$ contains an α^2 and at least four 1's. Recall that $r = 3$ divides $q - 1$, so $q \neq 2, 3$, which implies that $\alpha^2 \neq 1$. However, there is no such element in D by part (3) of Theorem 5.6, a contradiction. Hence $\pi(g)$ also fixes e_1, so $\pi(g) = 1$. Furthermore, there can be at most one element in the main diagonal of $g = \delta(g)$ which is different from 1, namely, that g_i, for which $u_i = e_2$. Using part (4) of Theorem 5.10 we get $g = 1$.

Finally, suppose that $|W| = 3$. First assume $\alpha^3 \neq 1$. If g is not a diagonal matrix, then

$$\delta(g) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \alpha & 0 \\ 0 & 0 & \alpha^{-1} \end{pmatrix} \text{ and } [\delta(g), s] = \begin{pmatrix} \alpha & 0 & 0 \\ 0 & \alpha^{-2} & 0 \\ 0 & 0 & \alpha \end{pmatrix}, \text{ for } s = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \in S.$$

Since $\alpha \neq \alpha^{-2}$, we have $[\delta(g), s] \notin D$ by part (3) of Theorem 5.6, which contradicts part (3) of Theorem 5.10. So g is a diagonal matrix.

If $\alpha^3 = 1$, that is, $q = 4$, then $\pi(C_G(u_1)) = 1$ by using the assumption $(|G|, |V|) = 1$, so g is again a diagonal matrix.

Since each basis element appears either in x or in y, $C_G(x) \cap C_G(y)$ cannot contain any diagonal matrix different from 1, which completes our proof. □

Still assuming that N is monomial, now we handle the case $r = 2$, that is, $n = 2^k$ for some k. If $n = 2$ then any $\mathbb{F}_q$-basis for V will do; for example, if $x = u_1$ and $y = u_2$ then $C_G(x) \cap C_G(y) = 1$. Now, we analyze the case $n = 4$. In accordance with Theorem 5.6, we choose a basis $\{u_1, u_2, u_3, u_4\} \subseteq V$. In this case $N = ZD_1S$, where the Klein 4-groups $D_1 = \langle d_2, d_3 \rangle$ and $S = \langle s_2, s_3 \rangle$ are generated

(independently from the base field) by the matrices:

$$d_2 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}, \quad d_3 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix},$$

$$s_2 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \quad s_3 = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}.$$

If the size of the base field is not equal to $3, 5$ or 9, then the following theorem guarantees the existence of a two-element base $\{x_0, y_0\} \subset V$. (For a more consistent notation, in the next two theorems the elements of the base are denoted by x_0, y_0 instead of x, y because they will be used in the constructions given for the case $n = 2^k,\ k \geq 3$.)

Theorem 5.13. *Let $N = Z\langle d_2, d_3, s_2, s_3\rangle \lhd G \leq GL(4, q)$, and assume that $q \neq 3, 5, 9$. Furthermore, let $\alpha \in \mathbb{F}_q^\times$ such that $\alpha^8 \neq 1$. Set $x_0 = u_1$ and $y_0 = u_2 + \alpha u_3 + \alpha^{-1} u_4$. Then $C_G(x_0) \cap C_G(y_0) = 1$.*

Proof. Let $g \in C_G(x_0) \cap C_G(y_0)$. Thanks to the choice of x_0 we know that g is a monomial matrix by Theorem 5.10 (1). The first element in the main diagonal of $\delta(g)$ is 1, and the others are from the set $\{1, \alpha, \alpha^{-1}, \alpha^2, \alpha^{-2}\}$. If $\delta(g)$ contains an α or an α^{-1}, then for some $s \in S$ we get $[\delta(g), s] \in D = Z \times D_1$ contains both α and α^{-1}. By part (3) of Theorem 5.6, this is impossible unless the order of α^2 divides 4, which is not the case. It follows that either $g = 1$, or

$$g = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & \alpha^2 \\ 0 & 0 & \alpha^{-2} & 0 \end{pmatrix} \qquad \text{and} \qquad [\delta(g), s_3] = \begin{pmatrix} \alpha^2 & 0 & 0 & 0 \\ 0 & \alpha^{-2} & 0 & 0 \\ 0 & 0 & \alpha^{-2} & 0 \\ 0 & 0 & 0 & \alpha^2 \end{pmatrix}.$$

In the latter case $[\delta(g), s_3] \in D$, so $o(\alpha^4)$ divides 2, which is again impossible. □

In the remaining cases we have found the following pair of vectors by using the GAP system [12].

Theorem 5.14. *Let $N = Z\langle d_2, d_3, s_2, s_3\rangle \leq GL(4, q)$ with $q \in \{3, 9, 5\}$ and let G be the normalizer of N in $GL(4, q)$. Depending on q, we define $x_0, y_0 \in V$ as follows*

(1) *Case $q = 3$:*

$$x_0 = u_1, \qquad y_0 = u_1 + u_3 + u_4.$$

Then for a suitable $3'$-Hall subgroup $H \leq G$ we have $C_H(x_0) \cap C_H(y_0) = 1$.

(2) *Case $q = 9$: Let α be a generator of the multiplicative group of $\mathbb{F}_9$ and*

$$x_0 = u_1 + u_3 + u_4, \qquad y_0 = u_2 + u_3 + \alpha u_4.$$

Then $C_G(x_0) \cap C_G(y_0) = 1$.

(3) *Case $q = 5$:*

$$x_0 = u_1 + u_2 + 2u_3, \qquad y_0 = u_2 + u_3 + 2u_4.$$

Then $C_G(x_0) \cap C_G(y_0) = 1$.

Remark 5.15. In case (1), G does not have a two-element base. Note that $|G| = 2^8 3^2$ in this case. If $G_1 \leq G$ is any $3'$-subgroup, then $g^{-1}G_1 g \leq H$ for some $g \in G$. By applying g to the basis elements we get $g(x_0),\ g(y_0)$ is a base for G_1.

The constructions given in the last two theorems have the common property that y_0 is a sum of exactly three basis vectors with non-zero coefficient. Using this observation, we shall give a uniform construction for $n = 2^k$ with $k \geq 3$.

We note that if $n \geq 128$ we could give similar constructions as we did in Theorem 5.12. However, for a more uniform approach we alter these constructions a bit, so they can be applied even in smaller dimensions. The point of our modification is that we do not choose x as a basis element this time, rather as a linear combination of exactly three basis vectors. Although this implies that $C_G(x)$ is no longer monomial, we can rectify this problem by an appropriate choice of y.

Again, let $\{e_1, e_2, \ldots, e_k\} \subseteq W = \{u_1, u_2, \ldots, u_n\}$ be a basis of W as an $\mathbb{F}_2$-vector space (see the paragraph before Theorem 5.11). Choosing the indexing of the basis vectors $u_1, u_2, \ldots, u_n$ appropriately, we can assume that

$$\langle e_1, e_2 \rangle_W = \{0, e_1, e_2, e_1 + e_2\} = \{u_1, u_2, u_3, u_4\}.$$

This results that $\{u_1, u_2, u_3, u_4\}$ corresponds to a two dimensional subspace of S.

Let $V' = \langle u_1, u_2, u_3, u_4 \rangle \leq V$ be the subspace generated by the first four basis vectors, and let $N_N(V')$ be the subgroup of elements of N fixing V' setwise. The restriction of $N_N(V')$ to V' defines an inclusion $N_N(V')/C_N(V')$ into $GL(V')$, so we get a subgroup $N' = Z \langle d_2, d_3, s_2, s_3 \rangle \leq GL(V')$. If $g \in N_G(V')$, then it is clear that $g_{V'}$ normalizes N'. Using the results of Theorem 5.13 and Theorem 5.14, we can define $x_0, y_0 \in V'$ such that y_0 is the linear combination of exactly three basis vectors and $N_G(V') \cap C_G(x_0) \cap C_G(y_0)$ acts trivially on V'. Starting from the vectors x_0, y_0, we search for a base $\{x, y\} \subseteq V$ of the form $x = y_0,\ y = x_0 + v$, where $v \in V'' := \langle u_5, u_6, \ldots, u_n \rangle$. The following lemma indicates why this form is useful.

Lemma 5.16. *$C_G(y_0)$ fixes both subspaces V' and V''. As a result, for any $v \in V''$ we have that $C_G(y_0) \cap C_G(x_0 + v) = C_G(y_0) \cap C_G(x_0) \cap C_G(v)$ acts trivially on V'. In particular, $C_G(y_0) \cap C_G(x_0 + v)$ consists of monomial matrices.*

Proof. First we prove the inclusion $C_G(y_0) \leq N_G(V') \cap N_G(V'')$. Our argument is similar to the way we have proved that $C_G(u_1)$ consists of monomial matrices in the proof of Theorem 5.10. As there are three basis elements in y_0 with non-zero coefficients and $S \simeq Z_2^k$ permutes the basis elements regularly, we get $C_N(y_0) \leq D$, i.e., every element of $C_N(y_0)$ is diagonal. Hence every element of $C_N(y_0)$ fixes the three basis elements appearing in y_0. Using the assumption that u_1, u_2, u_3, u_4 corresponds to a (two dimensional) subspace of S, it follows easily that any element of D fixing three of the basis elements u_1, u_2, u_3, u_4 must fix the fourth one, too. Let $M = C_N(y_0) = C_N(V')$ and let $V|_M$ denote the $\mathbb{F}_q M$-module V. It follows that $|D_1 : M| = 4$, so V' is just the homogeneous component of $V|_M$ corresponding to the trivial representation, while V'' is the sum of the other homogeneous components of $V|_M$. As $M \lhd C_G(y_0)$, every element of $C_G(y_0)$ permutes the homogeneous components of $V|_M$. Since $y_0 \in V'$, we get that $C_G(y_0)$ fixes V', so it also fixes the sum of the other homogeneous components of $V|_M$, which is V''.

Now, the inclusion $C_G(y_0) \cap C_G(x_0 + v) \supseteq C_G(y_0) \cap C_G(x_0) \cap C_G(v)$ is clear. For the reverse inclusion, let $g \in C_G(y_0) \cap C_G(x_0 + v)$. Note that $x_0 \in V',\ v \in V''$ and

$C_G(y_0)$ fixes setwise both subspaces V' and V''. Thus, $g(x_0) = x_0 + t,\ g(v) = v - t$ for some $t \in V' \cap V''$. But $V' \cap V'' = \{0\}$, which implies that $g(x_0) = x_0$ and $g(v) = v$.

Finally, we already proved that $g \in C_G(y_0) \cap C_G(x_0) \cap C_G(v)$ is an element of $N_G(V') \cap C_G(x_0) \cap C_G(y_0)$, which acts trivially on V' by the choice of x_0 and y_0. So g also fixes $u_1 \in V'$, hence g is a monomial matrix with respect to the basis $\{u_1, u_2, \ldots, u_n\}$ by Theorem 5.10. □

In view of the previous lemma, we can use part (3) of Theorem 5.11 to define a $\pi(C_G(x_0) \cap C_G(y_0))$-regular partition on W.

Theorem 5.17. *By using the displayed regular partitions P.3 and P.4 in the proof of Theorem 5.11 let $W = \{e_1\} \cup \{e_2\} \cup \Omega_3 \cup \Omega_4$ be a $\pi(C_G(x_0) \cap C_G(y_0))$-regular partition of $W = \{u_1, u_2, \ldots, u_n\}$. Let the vectors $x, y \in V$ be defined as*

$$\textit{For } |W| \neq 16: \quad x = y_0,\ y = x_0 + v, \qquad \textit{where } v = \sum_{u_i \in \Omega_4 \setminus \langle e_1, e_2 \rangle_W} u_i,$$

$$\textit{For } |W| = 16: \quad x = y_0,\ y = x_0 + v, \qquad \textit{where } v = 0e_3 + 2e_4 + \sum_{\substack{5 \leq i \leq 16 \\ u_i \notin \{e_3, e_4\}}} u_i.$$

Then we have $C_G(x) \cap C_G(y) = 1$.

Proof. Let $g \in C_G(x) \cap C_G(y)$. We know by the previous lemma that g is a monomial matrix fixing all elements of $\langle e_1, e_2 \rangle_W$.

If $|W| \neq 16$ then Ω_3 is fixed by $\pi(g)$, since $\Omega_3 \cup (\Omega_4 \setminus \langle e_1, e_2 \rangle_W) = W \setminus \langle e_1, e_2 \rangle_W$, and a basis element from $W \setminus \langle e_1, e_2 \rangle_W$ occurs with coefficient 0 in v if and only if it is an element of Ω_3. It follows that $\pi(g) = 1$. Hence $g = \delta(g)$ is a diagonal matrix, and any element in its main diagonal not corresponding to Ω_3 must be 1. Furthermore, since $|W| \neq 16$, $|\Omega_3| < \frac{1}{4}|W|$ by part (3) of Theorem 5.11, so we get $g = \delta(g) = 1$ by using part (4) of Theorem 5.10.

Now assume that $|W| = 16$, so $\pi(g)(e_3) = e_3$. Now, if $\pi(g)(e_4) \neq e_4$, then the number of elements in the main diagonal of $\delta(g)$ different from 1 is 2 or 3, which contradicts part (4) of Theorem 5.10. Hence $\delta(g) = 1$ and $\pi(g)(e_4) = e_4$. As e_1, e_2, e_3, e_4 is a base for the $\mathbb{F}_2$-space W, we get $g = \pi(g) = 1$, which proves the identity $C_G(x) \cap C_G(y) = 1$. □

5.3. **Finding a two-element base when N is non-monomial.** Now, we find a two element base when $Z \leq N \leq G$ is non-monomial. In agreement with Theorem 5.8 and the paragraph before it, we fix the notation as follows.

The whole space is denoted by U this time, so $G \leq GL(U)$. Now, $U = W \otimes V$, with respective bases $\{w_1, w_2\} \subseteq W$ and $\{u_1, u_2, \ldots, u_{n/2}\} \subseteq V$. We have $W_i = W \otimes \langle u_i \rangle$ and $V_j = \langle w_j \rangle \otimes V$ for each $1 \leq i \leq n/2,\ 1 \leq j \leq 2$, so

$$V = W_1 \oplus W_2 \oplus \ldots \oplus W_{n/2} = V_1 \oplus V_2.$$

Finally, N is decomposed as $N = (Q_8 \star D) \rtimes S$ with $N_1 = D \rtimes S \leq N_G(V_1)$. The restriction of $N_G(V_1)$ to V_1 yields a chain of subgroups $Z \leq N_1 \leq G_1 \leq GL(V_1) \simeq GL(V)$, with $G_1 \simeq N_G(V_1)/C_G(V_1)$.

As in the monomial case, the action of S defines a vector space structure on $\{u_1, u_2, \ldots, u_{n/2}\}$. Like we did in the paragraph before Lemma 5.16, we can assume

that $\{u_1, u_2, u_3, u_4\}$ forms a subspace in this space, i.e. it corresponds to a two dimensional subspace of S.

In the following theorem we give a summary of some of the results of Section 5.2 applied to the monomial case $Z \leq N_1 \leq G_1 \leq GL(V)$.

Theorem 5.18. *There are two vectors $x_1, y_1 \in V$ with the following properties*

(1) *If $g \in N_G(V_1)$ and $g \in C_G(w_1 \otimes x_1) \cap C_G(w_1 \otimes y_1)$, then $g_{V_1} = \mathrm{id}_{V_1}$.*
(2) *If $\dim V \geq 4$ then $x_1 \in \langle u_1, u_2, u_3, u_4 \rangle$ is a linear combination of exactly three basis vectors, while $y_1 \in u_1 + \langle u_5, \dots, u_{n/2} \rangle$.*
(3) *If $\dim V > 4$ then y_1 contains at least half of $u_1, \dots, u_{n/2}$ with non-zero coefficients.*

Proof. In fact, there is nothing new to prove, we just give references to our previous results here.

Part (1) only says that $x_1, y_1 \in V$ is a two-element base of the group $G_1 \leq GL(V)$. This was the goal of Section 5.2.

For $\dim V = 4$, part (2) follows from Theorem 5.13 and from part (1) of Theorem 5.14, with $x_1 = y_0$ and $y_1 = x_0$. (Note that $q \notin \{9, 5\}$ now, because $q \equiv -1 \mod 4$.)

For $\dim V > 4$, see Theorem 5.17. By choosing $x_1 = y_0$ and $y_1 = x_0 + v$, part (2) follows immediately. To see part (3), check that the number of u_i-s in y_1 is 4 for $\dim V = 8$, it is 12 for $\dim V = 16$, while it is $2^{k-1} - 2(k-1) > 2^{k-2}$ for $\dim V = 2^{k-1} \geq 32$. □

Theorem 5.19. *Using the vectors $x_1,\ y_1 \in V$ as in part (3) of Theorem 5.18 let*

$$x = w_1 \otimes u_1, \qquad y = w_2 \otimes u_1 + w_1 \otimes u_2, \qquad \text{for } \dim V = 2;$$
$$x = w_1 \otimes x_1 + w_2 \otimes u_1 \qquad y = w_1 \otimes y_1, \qquad \text{for } \dim V \geq 4.$$

Then $C_G(x) \cap C_G(y) = 1$.

Proof. First assume $\dim V = 2$, so $k = 2$. Let $g \in C_G(x) \cap C_G(y)$. Then g normalizes $C_N(x) = C_N(W_1) = D_1$, hence it permutes the homogeneous components of D_1, which are W_1, W_2 by part (2)(a) of Theorem 5.8. Since g fixes $x \in W_1$, it follows that g fixes setwise both W_1 and W_2. Using that g also fixes $y = w_2 \otimes u_1 + w_1 \otimes u_2$ we get that g fixes each of the vectors $w_1 \otimes u_1, w_2 \otimes u_1$ and $w_1 \otimes u_2$. Let $s \in S$ be a non-identity element of S. Then $[g, s] \in N$, and $[g, s](w_1 \otimes u_1) = w_1 \otimes u_1$. Thus, $[g, s] \in D$ and both restrictions $[g, s]_{W_1}$ and $[g, s]_{W_2}$ are scalar matrices. Then the same holds for g_{W_1} and g_{W_2}, so $g = 1$.

Now assume $\dim V = 4$, so $k = 3$ and $y_1 = u_1$ (see part (3)(b) in Theorem 5.18). Let $g \in C_G(x) \cap C_G(y)$. Then g normalizes $C_N(y) = C_N(w_1 \otimes u_1) = D_1$, hence it permutes its homogeneous components, that is, W_1, W_2, W_3, W_4. As $g(y) = y$, we also have $g(W_1) = W_1$. As x contains $w_2 \otimes u_1$ with non-zero coefficient, it follows that g acts trivially on W_1. Furthermore, g has a decomposition $\delta(g)\pi(g)$ with $\delta(g)$ fixing each W_1, W_2, W_3, W_4 and $\pi(g)$ permuting the basis elements. As in part (3) of Theorem 5.10, one can easily see that $[\delta(g), S] \subseteq Q_8 D$. The three basis vectors $w_1 \otimes u_i$ contained in x with non-zero coefficients are eigenvectors of $\delta(g)$, so $[\delta(g), s]$ has an eigenvector for any $s \in S$, thus $[\delta(g), S] \subseteq D$ by part (1) of Theorem 5.8. As $\delta(g)$ acts trivially on W_1 and S permutes W_1, W_2, W_3, W_4 in a transitive way, we get that $\delta(g)$ acts as a scalar matrix on each W_i. Hence g is a monomial matrix, so it fixes $V_1 = \langle w_1 \rangle \otimes V$. Then $g_{V_1} = \mathrm{id}_{V_1}$ by part (3)(a) of Theorem 5.18, and thus $g = 1$, as required.

Finally, let us assume that $\dim V > 4$. Let $U' = W_1 \oplus W_2 \oplus W_3 \oplus W_4$. First we claim that

$$C_N(x) = \{n \in N \mid n \text{ acts trivially on } U'\}.$$

As the set of subspaces W_1, W_2, W_3, W_4 corresponds to a 2-dimensional subspace of S and x is a linear combination of basis vectors with non-zero coefficients from three or four of the subspaces W_1, W_2, W_3, W_4, by using a similar argument as in Lemma 5.16 we get that $C_N(x)$ permutes the subspaces W_1, W_2, W_3, W_4. Now, for any $n \in C_N(x)$ there exist $w_1 \otimes u_s, w_1 \otimes u_t$ occurring in x with non-zero coefficients such that n moves $w_1 \otimes u_s$ to a multiple of $w_1 \otimes u_t$, so $w_1 \otimes u_t$ is an eigenvector of $\delta(n) \in Q_8 D$, hence $\delta(n) \in D$. It follows that $C_N(x) = C_N(w_1 \otimes x_1) \cap C_N(w_2 \otimes u_1)$. As $C_N(w_2 \otimes u_1) = D_1$, we get that $C_N(x)$ consists of diagonal matrices, so it fixes every basis element occurring in x with non-zero coefficients. Using again that each W_1, W_2, W_3, W_4 corresponds to a two dimensional subspace of S, we get that $C_N(x)$ acts trivially on U'. As $x \in U'$, the inclusion $C_N(U') \subseteq C_N(x)$ holds trivially.

Let $g \in C_G(x) \cap C_G(y)$. Then g normalizes $C_N(x)$, so it fixes the homogeneous component of $C_N(x)$ corresponding to the trivial representation of $C_N(x)$, which is exactly U', and the sum of the other homogeneous components, that is, $W_5 \oplus \ldots \oplus W_{n/2}$. Using the form of y_1, it follows that $g \in C_G(w_1 \otimes u_1)$. Therefore, $g(U') = U'$ and $g \in C_G(x) \cap C_G(w_1 \otimes u_1)$. Then $g_{U'} = \mathrm{id}_{U'}$ follows at once from the case $\dim V = 4$. As $g \in C_G(w_1 \otimes u_1)$, we get that g normalizes $D_1 = C_N(w_1 \otimes u_1)$, so g permutes $W_1, W_2, \ldots, W_{n/2}$. Let $g = \delta(g)\pi(g)$, where $\delta(g)$ fixes each of the subspaces $W_1, W_2, \ldots, W_{n/2}$, while $\pi(g)$ permutes the basis elements. More than half of the basis vectors $w_1 \otimes u_i,\ 1 \leq i \leq n/2$ are contained either in y, or in U', so $\delta(g)$ contains eigenvectors from more than half of the basis vectors $w_1 \otimes u_i,\ 1 \leq i \leq n/2$. (In fact, here we need to refer to U' only if $\dim V = 8$, since otherwise y itself contains more than half of the basis vectors $w_1 \otimes u_i$, see Theorem 5.17.) It follows that $[\delta(g), s]$ has an eigenvector for any $s \in S$, thus $[\delta(g), S] \subseteq D$. We now complete the proof as in the case $\dim V = 4$. □

Remark 5.20. In fact, it can be checked that in this section we only used the condition $(|G|, |V|) = 1$ in the cases $q = 4,\ n = 3$ and $q = 3,\ n = 2^k$. Moreover, it is clear that we can extend x_0, y_0 with some z_0 to a three element base of the full group G of symplectic type in part (1) of Theorem 5.14. By extending the vectors x, y in Theorems 5.17 and 5.19 with z_0 we get that even if the action is not coprime, a group $G \leq GL(2^k, 3)$ of symplectic type always has a base of size three.

6. Proof of Theorem 1.1

In this section we finish the proof of Theorem 1.1. In view of the results of Section 2, we investigate the case when V is an n-dimensional vector space over the field $\mathbb{F}_q$ of characteristic p and $Z \leq G \leq GL(V)$ is a coprime primitive (in particular, irreducible) linear group. We follow the strategy sketched at the end of Section 2.

First we prove a lemma which we will use to reduce the problem to the case where V is a sum of (isomorphic) absolutely irreducible $\mathbb{F}_q N$-modules for any $Z \leq N \lhd G$.

Lemma 6.1. *Let $G \leq \Gamma L(V)$ be a semilinear group such that $(|G|, |V|) = 1$ and let $H = G \cap GL(V)$. If $u_1, u_2 \in V$ is a base for H, then there exists $\gamma \in \mathbb{F}_q$ such that $u_1, u_2 + \gamma u_1$ is a base for G.*

Proof. For any $g \in G$ let $\sigma_g \in \mathrm{Gal}(\mathbb{F}_q|\mathbb{F}_p)$ denote the action of g on $\mathbb{F}_q$. For all $\alpha \in \mathbb{F}_q$ let $H_\alpha = C_G(u_1) \cap C_G(u_2 + \alpha u_1) \leq G$. Assuming that $C_H(u_1) \cap C_H(u_2) = 1$, our goal is to prove that $H_\alpha = 1$ for some $\alpha \in \mathbb{F}_q$. Let $g \in H_\alpha$. Thus, $g(u_1) = u_1$ and $u_2 + \alpha u_1 = g(u_2 + \alpha u_1) = g(u_2) + \alpha^{\sigma_g} u_1$. Hence $g(u_2) = u_2 + (\alpha - \alpha^{\sigma_g})u_1$. In particular, if $g \in \langle \cup H_\alpha \rangle$, then g is the product of elements from several H_α's, so $g(u_2) = u_2 + \delta u_1$ for some $\delta \in \mathbb{F}_q$.

We claim that $\langle \cup H_\alpha \rangle \cap H = 1$. Let $g \in \langle \cup H_\alpha \rangle \cap H$. On the one hand, the action of g on V is $\mathbb{F}_q$-linear, since $g \in H$. On the other hand, $g(u_1) = u_1$ and $g(u_2) = u_2 + \delta u_1$ for some $\delta \in \mathbb{F}_q$ by the previous paragraph. If $o(g) = m$, then $u_2 = g^m(u_2) = u_2 + m\delta u_1$, so $m\delta = 0$. Using that $|G|$ is coprime to p, we get m is not divisible by p, hence $\delta = 0$. Therefore, $g(u_2) = u_2$ and $g \in C_H(u_1) \cap C_H(u_2) = 1$.

Let g, h be two distinct elements of $\cup H_\alpha$, so $gh^{-1} \notin H$. Since G/H is embedded into $\mathrm{Gal}(\mathbb{F}_q|\mathbb{F}_p)$, we get $\sigma_g \neq \sigma_h$. Furthermore, the subfields of $\mathbb{F}_q$ fixed by σ_g and σ_h are the same if and only if $\langle g \rangle = \langle h \rangle$.

If $g \in H_\alpha \cap H_\beta$, then $g(u_2) = u_2 + (\alpha - \alpha^{\sigma_g})u_1 = u_2 + (\beta - \beta^{\sigma_g})u_1$, so $\alpha - \beta$ is fixed by σ_g. Let $K_g = \{\alpha \in \mathbb{F}_q \mid g \in H_\alpha\}$. The previous calculation shows that K_g is an additive coset of the subfield fixed by σ_g, so $|K_g| = p^d$ for some $d|f = \log_p q$. Since for any $d|f$ there is a unique p^d-element subfield of $\mathbb{F}_q$, we get $|K_g| \neq |K_h|$ unless the subfields fixed by σ_g and σ_h are the same. As we have seen, this means $\langle g \rangle = \langle h \rangle$. Consequently, $|K_g| \neq |K_h|$ unless $K_g = K_h$. Hence we get

$$\Big|\bigcup_{g \in \cup H_\alpha \setminus \{1\}} K_g\Big| \leq \sum_{d|f,\ d<f} p^d \leq \sum_{d<f} p^d = \frac{p^f - 1}{p - 1} < p^f = |\mathbb{F}_q|.$$

So there is a $\gamma \in \mathbb{F}_q$ which is not contained in K_g for any $g \in \cup H_\alpha \setminus \{1\}$. This exactly means that $H_\gamma = C_G(u_1) \cap C_G(u_2 + \gamma u_1) = 1$. □

Remark 6.2. In general, if $G \leq \Gamma L(V)$ is arbitrary and $H = G \cap GL(V)$, then $b(G) \leq b(H) + 1$, see [24, Lemma 3.2].

Now, we are ready to prove Theorem 1.1 for arbitrary coprime linear groups.

Proof of Theorem 1.1. First, we can assume that $G \leq GL(V)$ is a primitive (and thus irreducible) linear group by Theorem 2.6, where V is an n-dimensional vector space over $\mathbb{F}_q$. We will proceed by induction on $\dim V$; the base case $\dim V = 1$ is trivial.

Let $N \lhd G$ be a normal subgroup of G. Then V is a homogeneous $\mathbb{F}_q N$-module, so $V = V_1 \oplus V_2 \oplus \ldots \oplus V_k$, where the V_i's are isomorphic irreducible $\mathbb{F}_q N$-modules.

Suppose V_1 is not absolutely irreducible and let $T \simeq \mathrm{End}_{\mathbb{F}_q N}(V_1)$. By Schur's lemma, T is a proper field extension of $\mathbb{F}_q$, and

$$C_{GL(V)}(N) = \mathrm{End}_{\mathbb{F}_q N}(V) \cap GL(V) \simeq GL(k, T).$$

Furthermore, $L = Z(C_{GL(V)}(N)) \simeq Z(GL(k, T)) \simeq T^\times$. Now, by using L, we can extend V to a T-vector space of dimension $l := \dim_T V = \frac{\dim_{\mathbb{F}_q} V}{\dim_{\mathbb{F}_q} T} < \dim_{\mathbb{F}_q} V$. As $G \leq N_{GL(V)}(L)$, in this way we get an inclusion $G \leq \Gamma L(l, T)$. Using Lemma 6.1, we can assume that $G \leq GL(l, T)$. As $l = \dim_T V < \dim_{\mathbb{F}_q}(V)$, the result follows by induction. Hence, for the remainder of the proof we may assume that V is a direct sum of isomorphic absolutely irreducible $\mathbb{F}_q N$-modules for any $N \lhd G$.

Next, let $N \lhd G$ and let $V = V_1 \oplus \ldots \oplus V_k$ be a direct decomposition of V into isomorphic absolutely irreducible modules. By choosing a suitable basis in

$V_1, V_2, \ldots, V_k$, we can assume that $G \leq GL(n,q)$ such that any element of N is of the form $A \otimes I_k$ for some $A \in N_{V_1} \leq GL(n/k,q)$. By using [21, Lemma 4.4.3(ii)] we get

$$N_{GL(n,q)}(N) = \{B \otimes C \mid B \in N_{GL(n/k,q)}(N_{V_1}),\ C \in GL(k,q)\}.$$

Let

$$G_1 = \{g_1 \in GL(n/k,q) \mid \exists g \in G, g_2 \in GL(k,q) \text{ such that } g = g_1 \otimes g_2\}.$$

We define $G_2 \leq GL(k,q)$ in an analogous way. Then $G \leq G_1 \otimes G_2$. (Here G_1 and G_2 are not homomorphic images of G, since $g = g_1 \otimes g_2 = \lambda \cdot g_1 \otimes \lambda^{-1} g_2$ for any $\lambda \in \mathbb{F}_q^\times$, so the map $g = g_1 \otimes g_2 \mapsto g_1$ is not well-defined.) However, for any $g = g_1 \otimes g_2$ we have $g_1^{o(g)} = \lambda \cdot I_{n/k},\ g_2^{o(g)} = \lambda^{-1} \cdot I_k$ for some $\lambda \in \mathbb{F}_q^\times$, and thus $|G||\mathbb{F}_q^\times|$ is divisible by $o(g_1)$ and $o(g_2)$. It follows that $(|G_1|, p) = 1$ and $(|G_2|, p) = 1$. Suppose $1 < k < n$. Since $G_1 \leq GL(n/k,q)$ and $G_2 \leq GL(k,q)$, by induction we deduce that $b(G_1) \leq 2$ and $b(G_2) \leq 2$. In particular, by using Lemma 3.3 and [24, Lemma 3.3 (ii)] we have

$$b(G) \leq b(G_1 \otimes G_2) = b^*(G_1 \otimes G_2) \leq$$
$$\max(b^*(G_1), b^*(G_2)) = \max(b(G_1), b(G_2)) \leq 2.$$

Hence for the remainder we can assume that for any normal subgroup $N \lhd G$ either $N \leq Z = Z(G) \simeq \mathbb{F}_q^\times$ (and N consists of scalar matrices), or V is an absolutely irreducible $\mathbb{F}_q N$-module.

Let N be a normal subgroup of G such that N/Z is a minimal normal subgroup of G/Z. Then N/Z is a direct product of isomorphic simple groups. If N/Z is a direct product of cyclic groups of prime order, then G is of symplectic type. We examined such groups in Section 5, where we proved that $b(G) \leq 2$ for such a group.

In the following let N/Z be a direct product of $t \geq 2$ isomorphic non-Abelian simple groups. Then $N = L_1 \star L_2 \star \ldots \star L_t$ is a central product of isomorphic groups such that for every $1 \leq i \leq t$ we have $Z \leq L_i,\ L_i/Z$ is simple. Furthermore, conjugation by elements of G permutes the subgroups $L_1, L_2, \ldots, L_t$ in a transitive way. By choosing an irreducible $\mathbb{F}_q L_1$-module $V_1 \leq V$, and a set of coset representatives $g_1 = 1, g_2, \ldots, g_t \in G$ of $G_1 = N_G(V_1)$ such that $L_i = g_i L_1 g_i^{-1}$, we get that $V_i := g_i V_1$ is an absolutely irreducible $\mathbb{F}_q L_i$-module for each $1 \leq i \leq t$. Now, $V \simeq V_1 \otimes V_2 \otimes \ldots \otimes V_t$ by [26, Corollary 18.2(a)] and G permutes the factors of this tensor product. It follows that G is embedded into the central wreath product $G_1 \wr_c S_t$. By induction we have $b(G_1) \leq 2$, so Theorem 3.8 implies that $b(G) \leq 2$ if $t \geq 2$.

Finally, let $Z \leq N \lhd G$ be such that N/Z is a non-Abelian simple group. Then $N_1 = [N, N] \lhd G$ is a quasisimple group. Let $\mathbb{F}_p$ be the prime field of $\mathbb{F}_q$. Viewing V as an $\mathbb{F}_p G$-module it decomposes into a sum of isomorphic irreducible $\mathbb{F}_p N_1$-modules. Let V_1 be an irreducible $\mathbb{F}_p N_1$-submodule of V and

$$G_1 = \{g \in G \mid g(V_1) = V_1\}$$

be the stabilizer of V_1. Then there is a homomorphism $\varphi : G_1 \to GL(V_1)$ which is faithful on N_1. Therefore, $\ker\varphi \cap N_1 = 1$, so $\ker\varphi \leq C_G(N_1) = C_G(N_1 Z) = C_G(N) = Z$. As any non-identity element of Z acts on $V \setminus \{0\}$ fixed point freely, we get $\ker\varphi = 1$, so we may view G_1 as a subgroup of $GL(V_1)$. Therefore, we have the situation $N_1 \lhd G_1 \leq GL(V_1)$, with $(|G_1|, |V_1|) = 1$ and V_1 is a vector space over the prime field $\mathbb{F}_p$. Moreover, N_1 is quasisimple and V_1 is irreducible as an

$\mathbb{F}_pN_1$-module. By using the results of Section 4 there exist $x, y \in V_1 \leq V$ such that $C_{G_1}(x) \cap C_{G_1}(y) = 1$. Let $g \in C_G(x) \cap C_G(y)$ and let $N_1x = \{nx \mid n \in N_1\}$. Then $gnx = gng^{-1}gx = gng^{-1}x \in N_1x$ for any $n \in N_1$, so N_1x is a g-invariant subset. As the $\mathbb{F}_p$-subspace generated by N_1x is exactly V_1, we get that V_1 is g-invariant, that is, $g \in G_1$. This proves that $C_G(x) \cap C_G(y) = C_{G_1}(x) \cap C_{G_1}(y) = 1$. So $b(G) \leq 2$, which completes our proof. □

Acknowledgement. The authors are very grateful to L. Pyber for bringing our attention to the papers [15] and [22]. Without this information it is very unlikely that we would have been able to handle the almost quasisimple case. We also thank P. P. Pálfy for his helpful comments, especially for providing us with a much simpler proof than our original one for handling Case 3 of Theorem 4.4. We are also very grateful to A. Maróti and to the anonymous referee for their many comments and suggestions.

References

1. M. Aschbacher, *Finite group theory, 2nd ed.* Cambridge Studies in Advanced Mathematics 10, Cambridge University Press (2000).
2. C. Benbenishty, *On actions of primitive groups*, PhD thesis, Hebrew University, Jerusalem, 2005.
3. T. C. Burness, *On base sizes for actions of finite classical groups*, J. Lond. Math. Soc. **75** (2007), 545–562.
4. T. C. Burness, R. M. Guralnick and J. Saxl, *On base sizes for symmetric groups*, Bull. Lond. Math. Soc. **43** (2011), 386–391.
5. T. C. Burness, M. W. Liebeck and A. Shalev, *Base sizes for simple groups and a conjecture of Cameron*, Proc. Lond. Math. Soc. **98** (2009), 116–162.
6. T. C. Burness, E. A. O'Brien and R. A. Wilson, *Base sizes for sporadic simple groups*, Israel J. Math. **177** (2010), 307–333.
7. T. C. Burness and Á. Seress, *On Pyber's base size conjecture*, to appear in Trans. Amer. Math. Soc. (2013)
8. J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker and R. A. Wilson, *Atlas of finite groups*, Oxford University Press, 1985.
9. S. Dolfi, *Orbits of permutation groups on the power set*, Arch. Math. **75** (2000) 321–327.
10. S. Dolfi, *Large orbits in coprime actions of solvable groups*, Trans. Amer. Math. Soc. **360** (2008), 135–152.
11. J. B. Fawcett, *The base size of a primitive diagonal group*, J. Algebra **375** (2013), 302–321.
12. The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.4.10*; 2007. (http://www.gap-system.org)
13. D. Gluck, *Trivial set-stabilizers in finite permutation groups*, Canad. J. Math. **35** (1983), 59–67.
14. D. Gluck and K. Magaard, *Base sizes and regular orbits for coprime affine permutation groups*, J. Lond. Math. Soc. (2) **58** (1998), 603–618.
15. D. P. M. Goodwin, *Regular orbits of linear groups with an application to the k(GV)-problem*, I,II. J. Algebra **227** (2000), 395–432 and 433–473.
16. Z. Halasi and A. Maróti, *The minimal base size for a p-solvable linear group*, arXiv:1310.5454 (2013)
17. B. Hartley and A. Turull, *On characters of coprime operator groups and the Glauberman character correspondence*, J. Reine Angew. Math. **451** (1994), 175–219.
18. B. Huppert, *Endliche Gruppen. I.* Die Grundlehren der Mathematischen Wissenschaften, Band 134 Springer-Verlag, Berlin-New York, 1967.
19. I. M. Isaacs, *Character theory of finite groups*, Dover, New York, 1994.
20. I. M. Isaacs, *Large orbits in actions of nilpotent groups*, Proc. Amer. Math. Soc. **127** (1999) 45–50.
21. P. Kleidman and M. W. Liebeck, *The Subgroup Structure of the Finite Classical Groups*, London Math. Soc. Lecture Note Series, Vol. 129, Cambridge University Press, 1990.

22. C. Köhler and H. Pahlings, *Regular orbits and the $k(GV)$-problem*, Groups and computation, III, (Columbus, OH, 1999), Ohio State Univ. Math. Res. Inst. Publ. **8**, de Gruyter, Berlin (2001), 209–228.
23. M. W. Liebeck and A. Shalev, *Simple groups, permutation groups, and probability*, J. Amer. Math. Soc. **12** (1999) 497–520.
24. M. W. Liebeck and A. Shalev, *Bases of primitive linear groups*, J. Algebra **252** (2002) 95–113.
25. G. Malle and G. Navarro, *Blocks with equal height zero degrees*, Trans. Amer. Math. Soc. **363** (2011), 6647–6669.
26. G. Malle and D. Testerman, *Linear algebraic groups and finite groups of Lie type*, Cambridge Studies in Advanced Mathematics 133, Cambridge University Press, 2011.
27. A. Moreto and T. R. Wolf, *Orbit sizes, character degrees and Sylow subgroups*, Adv. Math. **184** (2004) 18–36.
28. D. S. Passman, *Groups with normal solvable Hall p'-subgroups*, Trans. Amer. Math. Soc. **123** (1966), 99–111.
29. P. P. Pálfy and L. Pyber, *Small groups of automorphisms*, Bull. Lond. Math. Soc. **30** (1998) 386–390.
30. L. Pyber, *Asymptotic results for permutation groups*, Groups and computation, DIMACS Ser. Discrete Math. Theoret. Comp. Sci. **11** Amer. Math. Soc., Providence, RI, (1993) 197–219.
31. Á. Seress, *The minimal base size of primitive solvable permutation groups*, J. Lond. Math. Soc. **53** (1996) 243–255.
32. Á. Seress, *Primitive groups with no regular orbits on the set of subsets*, Bull. Lond. Math. Soc. **29**, 697–704 (1997).
33. Á. Seress, *Permutation Group Algorithms*, Cambridge Tracts in Mathematics. 152, Cambridge University Press, 2003.
34. E. P. Vdovin, *Regular orbits of solvable linear p'-groups*, Sib. Èlektron. Mat. Izv. **4** (2007), 345–360.
35. T. R. Wolf, *Large orbits of supersolvable linear groups*, J. Algebra **215** (1999) 235–247.

Institute of Mathematics, University of Debrecen, P. O. Box 12, H-4010 Debrecen, Hungary

E-mail address: halasi.zoltan@renyi.mta.hu

Budapest Business School, College of Finance and Accountancy, Buzogány street 10-12, H-1149 Budapest, Hungary

E-mail address: podoski.karoly@pszfb.bgf.hu