# THE MINIMAL BASE SIZE FOR A $p$-SOLVABLE LINEAR GROUP

ZOLTÁN HALASI AND ATTILA MARÓTI

ABSTRACT. Let $V$ be a finite vector space over a finite field of order $q$ and of characteristic $p$. Let $G \leq GL(V)$ be a $p$-solvable completely reducible linear group. Then there exists a base for $G$ on $V$ of size at most 2 unless $q \leq 4$ in which case there exists a base of size at most 3. The first statement extends a recent result of Halasi and Podoski and the second statement generalizes a theorem of Seress. An extension of a theorem of Pálfy and Wolf is also given.

*Dedicated to the memory of Ákos Seress.*

## 1. Introduction

For a finite permutation group $H \leq \mathrm{Sym}(\Omega)$, a subset of the finite set $\Omega$ is called a base, if its pointwise stabilizer in $H$ is the identity. The minimal base size of $H$ (on $\Omega$) is denoted by $b(H)$. Notice that $|H| \leq |\Omega|^{b(H)}$.

One of the highlights of the vast literature on base sizes of permutation groups is the celebrated paper of Á. Seress [18] in which it is proved that $b(H) \leq 4$ whenever $H$ is a solvable primitive permutation group. Since a solvable primitive permutation group is of affine type, this result is equivalent to saying that a solvable irreducible linear subgroup $G$ of $GL(V)$ has a base of size at most 3 (in its natural action on $V$) where $V$ is a finite vector space.

There are a number of results on base sizes of linear groups. For example, D. Gluck and K. Magaard [8, Corollary 3.3] have shown that a subgroup $G$ of $GL(V)$ with $(|G|, |V|) = 1$ admits a base of size at most 94. If in addition it is assumed that $G$ is supersolvable or of odd order then $b(G) \leq 2$ by results of T.R. Wolf [21, Theorem A] and S. Dolfi [4, Theorem 1.3]. Later S. Dolfi [5, Theorem 1.1] and E.P. Vdovin [19, Theorem 1.1] generalized this result to solvable coprime linear groups. Finally, Z. Halasi and K. Podoski [10, Theorem 1.1] improved this result significantly, by proving that even the solvability assumption can be dropped, and $b(G) \leq 2$ for any coprime linear group $G$.

The research of the first author leading to these results has received funding from the European Union's Seventh Framework Programme (FP7/2007-2013) under grant agreement no. 318202, from ERC Limits of discrete structures Grant No. 617747 and from OTKA K84233. The research of the second author was supported by a Marie Curie International Reintegration Grant within the 7th European Community Framework Programme, by an Alexander von Humboldt Fellowship for Experienced Researchers, by the János Bolyai Research Scholarship of the Hungarian Academy of Sciences, by OTKA K84233, and by the MTA RAMKI Lendület Cryptography Research Group.

We note that for a solvable subgroup $G$ of $GL(V)$ acting completely reducibly on $V$ we have $b(G) \leq 2$ if the Sylow 2-subgroups of $GV$ are Abelian (see [6, Theorem 2]) or if $|G|$ is not divisible by 3 (see [22, Theorem 2.3]).

The following definition has been introduced by M. W. Liebeck and A. Shalev in [14]. For a linear group $G \leq GL(V)$ we say that $\{v_1, \ldots, v_k\} \subseteq V$ is a strong base for $G$ if any element of $G$ fixing $\langle v_i \rangle$ for every $1 \leq i \leq k$ is a scalar transformation. The minimal size of a strong base for $G$ is denoted by $b^*(G)$. It is known that $b(G) \leq b^*(G) \leq b(G) + 1$ (see [14, Lemma 3.1]). Furthermore, also $b^*(G) \leq 2$ holds for coprime linear groups by [10, Lemma 3.3 and Theorem 1.1].

The following theorem extends the above-mentioned result of Seress [18] and that of Halasi and Podoski to $p$-solvable groups.

**Theorem 1.1.** *Let $V$ be a finite vector space over a field of order $q$ and of characteristic $p$. If $G \leq GL(V)$ is a $p$-solvable group acting completely reducibly on $V$, then $b^*(G) \leq 2$ unless $q \leq 4$. Moreover if $q \leq 4$ then $b^*(G) \leq 3$.*

One of the motivations of Seress [18] was a famous result of P.P. Pálfy [16, Theorem 1] and Wolf [20, Theorem 3.1] stating that a solvable primitive permutation group of degree $n$ has order at most $24^{-1/3} n^d$ where $d = 1 + \log_9(48 \cdot 24^{1/3}) = 3.243\ldots$, that is to say, a solvable irreducible subgroup $G$ of $GL(V)$ has size at most $24^{-1/3}|V|^{d-1}$. (This bound is attained for infinitely many groups.) In the following we extend this result to $p$-solvable linear groups $G$.

**Theorem 1.2.** *Let $V$ be a finite vector space over a field of characteristic $p$. If $G \leq GL(V)$ is a $p$-solvable group acting completely reducibly on $V$, then $|G| \leq 24^{-1/3}|V|^{d-1}$ where $d$ is as above.*

We note that the bounds in Theorem 1.1 are best possible for all values of $q$. Indeed, there are infinitely many irreducible solvable linear groups $G \leq GL(V)$ with $|G| > |V|^2$ for $q = 2$ or $3$ (see [16, Theorem 1] or [20, Proposition 3.2]) and there are even infinitely many odd order completely reducible linear groups $G \leq GL(V)$ with $|G| > |V|$ for $q \geq 5$ (see [17, Theorem 3B] and the remark that follows). For $q = 4$ we note that there are primitive, irreducible solvable linear subgroups $H$ of $GL(3,4)$ with $b(H) = 3$ and thus there are infinitely many imprimitive, irreducible solvable linear groups $G = H \wr S \leq GL(3r, 4)$ with $b(G) = 3$ where $S$ is a solvable transitive permutation group of degree $r$.

Theorem 1.1 has been applied in [2] to Gluck's conjecture.

## 2. Preliminaries

Throughout this paper let $\mathbb{F}_q$ be a finite field of characteristic $p$ and let $V$ be an $n$-dimensional vector space over $\mathbb{F}_q$. Furthermore, let $G \leq GL(V)$ be a linear group acting on $V$ in the natural way, let $b(G)$ denote its minimal base size, and let $b^*(G)$ denote its minimal strong base size (both notions defined in Section 1).

If the vector space $V$ is fixed, then the group of scalar transformations of $V$ (the center of $GL(V)$) will be denoted by $Z$. Thus $Z \simeq \mathbb{F}_q^\times$, the multiplicative group of the base field. As $G \leq GL(V)$ is $p$-solvable if and only if $GZ$ is $p$-solvable, we can (and we will) always assume, in the proofs of Theorems 1.1 and 1.2, that $G$

contains $Z$. After choosing a basis $\{v_1, \ldots, v_n\} \subseteq V$, we will always identify the group $GL(V)$ with the group $GL(n, q)$.

Put $t(q) = 3$ for $q \leq 4$ and $t(q) = 2$ for $q \geq 5$.

Finally, if $G \leq GL(V)$ and $X \subseteq V$, then $C_G(X) = \{g \in G \mid g(x) = x \ \forall x \in X\}$ and $N_G(X) = \{g \in G \mid g(x) \in X \ \forall x \in X\}$ will denote the pointwise and setwise stabilizer of $X$ in $G$, respectively.

## 3. Special bases in linear groups

In this section we will show that there exist bases of special kinds for certain linear groups. As a consequence (Corollary 3.3), we derive that it is sufficient to establish the required bounds in Theorem 1.1 for $b(G)$ rather than for $b^*(G)$.

**Theorem 3.1.** *Let $V$ be an $n$-dimensional vector space over $\mathbb{F}_q$, a field of characteristic $p$ and let $Z \leq G \leq GL(V)$ be a $p$-solvable linear group.*

*(1) If $n = 2$ and $q \geq 5$, then at least one of the following holds.*
  - *(a) There is a basis $x, y \in V$ such that $N_G(\langle x \rangle) \subseteq N_G(\langle y \rangle)$.*
  - *(b) $p = 2$ and there is a basis $x, y \in V$ such that $N_G(\langle x \rangle) = Z \times C_2$ and the involution $g$ in $N_G(\langle x \rangle)$ satisfies $g(x) = x$ and $g(y) = y + x$.*

*(2) If $n = 3$ and $q = 3$ or $4$, then at least one of the following holds.*
  - *(a) There is a basis $x, y, z \in V$ such that $N_G(\langle x \rangle) \cap N_G(\langle y \rangle) \subseteq N_G(\langle z \rangle)$.*
  - *(b) There is a basis $x, y, z \in V$ such that $N_G(\langle y, z \rangle) = G$.*

*Proof.* Firstly we may assume that $G$ is an irreducible primitive subgroup of $GL(V)$. Since $G$ is $p$-solvable by assumption, we see that $G$ does not contain $SL(V)$.

First consider statement (1). By considering the action of $G$ on the set $S$ of 1-dimensional subspaces of $V$, we may assume that the number of Sylow $p$-subgroups of $G$ is equal to $|S| = q + 1$. For otherwise there exists $\langle x \rangle \in S$ whose stabilizer in $G$ is a $p'$-group and thus Maschke's theorem gives 1/(a). For $q = p$ any subgroup of $GL(V)$ with $q + 1$ Sylow $p$-subgroups contains $SL(V)$, so in this case we are done. So assume that $q > p$.

Since $G$ acts transitively on the set of Sylow $p$-subgroups of $G$ and every Sylow $p$-subgroup stabilizes a unique subspace in $S$, it follows that $G$ acts transitively on $S$. Moreover since $Z \leq G$ it also follows that $G$ acts transitively on the set of non-zero vectors of $V$.

By Hering's theorem (see [11, Chapter XII, Remark 7.5 (a)]) we see that if $q$ is odd (and not a prime by assumption) then $q$ must be 9 and $G$ has a normal subgroup isomorphic to $SL(2, 5)$ (case (5)). But then $G$ is not 3-solvable and so we can rule out this possibility. Similarly, if $q$ is even, then the only possibility is that $G \geq Z$ normalizes a Singer cycle $GL(1, q^2)$ (case (1)). The only such group not satisfying 1/(a) is the full semilinear group $\Gamma(1, q^2) \simeq GL(1, q^2).2$. In this case taking $x$ to be any non-zero vector in $V$ we have $N_G(\langle x \rangle) = Z \times C_2$ and the involution $g$ in $N_G(\langle x \rangle)$ satisfies $g(x) = x$ and $g(y) = y + x$ for some $y \in V$.

Finally, statement (2) has been checked with GAP [7] by using the list of all primitive permutation groups of degrees 27 and 64, respectively. □

As a direct consequence we get the following.

**Corollary 3.2.** *Let us assume that $Z \leq G \leq GL(V)$ is a $p$-solvable linear group with $b(G) \leq t(q)$.*

(1) *If $q \geq 5$, then one of the following holds.*
  (a) *There exists a base $x, y \in V$ such that $N_G(\langle x \rangle) \cap N_G(\langle x, y \rangle) \subseteq N_G(\langle y \rangle)$.*
  (b) *$p = 2$ and there exists a base $x, y \in V$ such that any non-identity element of $C_G(x) \cap N_G(\langle x, y \rangle)$ takes $y$ to $y + x$.*

(2) *If $q \leq 4$, then at least one of the following holds.*
  (a) *There exists a base $x, y, z \in V$ such that*
$$N_G(\langle x \rangle) \cap N_G(\langle y \rangle) \cap N_G(\langle x, y, z \rangle) \subseteq N_G(\langle z \rangle).$$
  (b) *There exists a base $x, y, z \in V$ such that $N_G(\langle x, y, z \rangle) \subseteq N_G(\langle y, z \rangle)$ with $x \notin \langle y, z \rangle$.*

*Proof.* First, 1/(a) or 2/(a) holds if $\dim(V) < t(q)$ so assume that $\dim(V) \geq t(q)$. Both parts of the corollary can be proved by choosing a subspace $U \leq V$ of dimension $t(q)$ generated by a base for $G$ and by restricting $N_G(U)$ to this subspace. Notice that the image of this restriction is also $p$-solvable, so Theorem 3.1 can be applied. □

**Corollary 3.3.** *Let $V$ be a vector space over the field $\mathbb{F}_q$ of characteristic $p$. Let $Z \leq G \leq GL(V)$ be $p$-solvable with $b(G) \leq t(q)$. Then $b^*(G) \leq t(q)$.*

*Proof.* We may assume that $\dim(V) \geq t(q)$ and that $q > 2$. Let us choose a base for $G$ of size $t(q)$ satisfying the property given in Corollary 3.2. For $q \geq 5$, if $x, y \in V$ is such a base, then $x, x + y$ is a strong base for $G$. Likewise, for $q = 3$ or 4, if $x, y, z \in V$ is a base satisfying (2/a) of Corollary 3.2, then $x, y, x + y + z$ is a strong base for $G$. Finally, in case $x, y, z \in V$ is a base for $G$ satisfying (2/b) of Corollary 3.2, then $x, y + x, z + x$ is a strong base for $G$. □

## 4. Further reductions

Let us use induction on the dimension $n$ of $V$ in the proofs of Theorems 1.1 and 1.2. The case $n = 1$ is clear. Let us assume that $n > 1$ and that both Theorems 1.1 and 1.2 are true for dimensions less than $n$.

First we reduce the proof of both theorems for the case when $G \leq GL(V)$ acts irreducibly on $V$. For otherwise let $V = V_1 \oplus V_2 \oplus \ldots \oplus V_k$ be a decomposition of $V$ to irreducible $\mathbb{F}_q G$-modules.

By induction, there exist vectors $x_{i,1}, \ldots, x_{i,t(q)}$ in $V_i$ for $1 \leq i \leq k$ with the property that $C_G(\{x_{i,1}, \ldots, x_{i,t(q)}\})$ is precisely the kernel of the action of $G$ on $V_i$. Now put $x_j = \sum_{i=1}^{k} x_{i,j}$ for $1 \leq j \leq t(q)$. One can see that $C_G(\{x_1, \ldots, x_{t(q)}\}) = \cap_{i=1}^{k} C_G(V_i) = 1$.

For Theorem 1.2 notice that $G$ is a subgroup of a direct product $\times_{i=1}^{k} H_i$ of $p$-solvable groups $H_i$ acting irreducibly and faithfully on the $V_i$'s. Hence we have
$$|G| \leq \prod_{i=1}^{k} |H_i| \leq \prod_{i=1}^{k} \left( 24^{-1/3} |V_i|^{d-1} \right) = 24^{-k/3} |V|^{d-1}$$
by induction.

So from now on we will assume that $G \leq GL(V)$ acts irreducibly on $V$.

For Theorem 1.1 we may also assume that $q \neq 2$, 4. Otherwise, $G$ is solvable by the Odd Order Theorem and we can use the result of Seress [18].

For Theorem 1.2 we may assume that $|G| > |V|^2$. If $|G| \leq |V|^2$ then $|V|^2 < 24^{-1/3}|V|^{d-1}$ for $|V| \geq 79$, so we may assume that $|V| \leq 73$. If $|V|$ is a prime or $p = 2$ then $G$ is solvable and the theorem of Pálfy [16] and Wolf [20] can be applied. Hence the cases $|V| = 5^2, 7^2, 3^2$ or $3^3$ remain to be examined. But in these cases there is no non-solvable, $p$-solvable irreducible subgroup of $GL(V)$ (see [7]).

Now, if $b(G) \leq 2$ then $|G| \leq |V|^2$. So, once Theorem 1.1 is proved, it remains to prove Theorem 1.2 only in case $q = 3$ and $b(G) > 2$.

## 5. Imprimitive linear groups

In this section we show that we may assume (for the proofs of Theorems 1.1 and 1.2) that $G$ is a primitive (irreducible) subgroup of $GL(V)$.

We first consider Theorem 1.1.

For $G \leq GL(V)$ an irreducible imprimitive linear group, let $V = V_1 \oplus \cdots \oplus V_k$ be a decomposition of $V$ into subspaces such that $G$ permutes these subspaces in a transitive and primitive way. This action of $G$ defines a homomorphism from $G$ into the symmetric group $\mathrm{Sym}(\Omega)$ for $\Omega = \{V_1, \ldots, V_k\}$ with kernel $N$.

The factor group $G/N \leq S_k$ is $p$-solvable, so it does not involve $A_q$ for $q \geq 5$ and it does not involve $A_5$ for $q = 3$. By using [10, Theorem 2.3] it follows that for $q \geq 5$ there is a vector $a = (a_1, \ldots, a_k) \in \mathbb{F}_q^k$ such that $C_{G/N}(a) = 1$, while for $q = 3$ there is a pair of vectors $a = (a_1, \ldots, a_k),\ b = (b_1, \ldots, b_k) \in \mathbb{F}_3^k$ such that $C_{G/N}(a) \cap C_{G/N}(b) = 1$. (Here, $G/N$ acts on $\mathbb{F}_q^k$ by permuting coordinates.)

In fact for $q \geq 8$ even we can say a bit more. For such a $q$ let $S$ be a subset of $\mathbb{F}_q$ of size $q/2$ with the property that for each $c \in \mathbb{F}_q$ exactly one of $c$ and $c+1$ is contained in $S$. By [3, Lemma 1/(c)] there exists a vector $a = (a_1, \ldots, a_k) \in S^k$ such that $C_{G/N}(a) = 1$.

For each $1 \leq i \leq k$ let $H_i = N_G(V_i)$, so $N = \cap_i H_i$. By induction (on the dimension), there is a base in $V_1$ of size $t(q)$ for $H_1/C_{H_1}(V_1)$.

Now we can use Corollary 3.2. First let $q \geq 5$. Then there is a base $x_1, y_1 \in V_1$ for $K_1 = H_1/C_{H_1}(V_1) \leq GL(V_1)$ such that $N_{K_1}(\langle x_1 \rangle) \cap N_{K_1}(\langle x_1, y_1 \rangle) \subseteq N_{K_1}(\langle y_1 \rangle)$ or that any non-identity element of $C_{K_1}(x_1) \cap N_{K_1}(\langle x_1, y_1 \rangle)$ takes $y_1$ to $y_1 + x_1$.

Let $\{g_1 = 1, g_2, \ldots, g_k\}$ be a set of left coset representatives for $H_1$ in $G$ and $x_i = g_i x_1,\ y_i = g_i y_1$ for every $i$. Now let

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

In case $q = 3$ let $x_1, y_1, z_1 \in V_1$ be a base for $K_1 = H_1/C_{H_1}(V_1) \leq GL(V_1)$ satisfying (2/a) or (2/b) of Corollary 3.2. Again, let $\{g_1 = 1, g_2, \ldots, g_k\}$ be a set of left coset representatives for $H_1$ in $G$ and $x_i = g_i x_1,\ y_i = g_i y_1,\ z_i = g_i z_1$ for every $i$. Depending on which part of part (2) of Corollary 3.2 is satisfied for $x_1, y_1, z_1$ let

$$x = \sum_{i=1}^{k} x_i, \qquad y = \sum_{i=1}^{k} y_i \qquad z = \sum_{i=1}^{k} (z_i + b_i x_i + a_i y_i) \quad \text{if (2/a) holds,}$$
$$x = \sum_{i=1}^{k} x_i, \qquad y = \sum_{i=1}^{k} (y_i + a_i x_i) \qquad z = \sum_{i=1}^{k} (z_i + b_i x_i) \quad \text{if (2/b) holds.}$$

In each case, it is easy to see that the given set of vectors is a base for $G$ by using similar arguments as in the proof of [10, Theorem 2.6].

Now we turn to the reduction of Theorem 1.2 to primitive groups. Notice that $N$ is a $p$-solvable group and $V$ is the sum of at least $k$ irreducible $\mathbb{F}_q N$-modules, so we have $|N| \leq 24^{-k/3} |V|^{d-1}$ by Section 4. Since the permutation group $G/N \leq S_k$ is 3-solvable, it does not contain any non-Abelian alternating composition factor, and so $|G/N| \leq 24^{(k-1)/3}$, by [15, Corollary 1.5]. But then $|G| = |N||G/N| \leq 24^{-1/3} |V|^{d-1}$ which is exactly what we wanted.

## 6. Groups of semilinear transformations

In this section we reduce Theorems 1.1 and 1.2 to the case when every irreducible $\mathbb{F}_q N$-submodule of $V$ is absolutely irreducible for any normal subgroup $N$ of $G$.

For this purpose let $N \lhd G$ be a normal subgroup of $G$. Then $V$ is a homogeneous $\mathbb{F}_q N$-module, so $V = V_1 \oplus V_2 \oplus \cdots \oplus V_k$, where the $V_i$'s are isomorphic irreducible $\mathbb{F}_q N$-modules. Let $T := \mathrm{End}_{\mathbb{F}_q N}(V_1)$. Assuming that the $V_i$'s are not absolutely irreducible, $T$ 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 $l := \dim_T V < \dim_{\mathbb{F}_q} V$. As $G \leq N_{GL(V)}(L)$, in this way we get an inclusion $G \leq \Gamma L(l, T)$. We proceed by proving the following theorem.

**Theorem 6.1.** *For a proper field extension $T$ of $\mathbb{F}_q$ let $G \leq \Gamma L(l, T)$ be a semilinear group acting on the $\mathbb{F}_q$-space $V$ and let $H = G \cap GL(l, T)$. Suppose that $G$ is $p$-solvable and that $b(H) \leq t(|T|)$. Then $b(G) \leq t(|T|)$.*

*Proof.* We modify the proof of [10, Lemma 6.1] to make it work in this more general setting.

Clearly we may assume that $|T| \geq 8$ is different from a prime. In these cases $t(|T|) = 2$.

Let $u_1, u_2$ be a base for $H$. By Corollary 3.2, we may also assume that

$$N_H(\langle u_1 \rangle) \cap N_H(\langle u_1, u_2 \rangle) \subseteq N_H(\langle u_2 \rangle)$$

or that every non-identity element of $C_H(u_1) \cap N_H(\langle u_1, u_2 \rangle)$ takes $u_2$ to $u_2 + u_1$. (The latter case occurs only if $p = 2$.)

For every $\alpha \in T$ let $H_\alpha = C_G(u_1) \cap C_G(u_2 + \alpha u_1) \leq G$. Our goal is to prove that $H_\alpha = 1$ for some $\alpha \in T$. If $g \in \langle \cup H_\alpha \rangle$, then $g(u_1) = u_1$ and $g(u_2) = u_2 + \delta u_1$ for some $\delta \in T$.

We claim that $|\langle \cup H_\alpha\rangle \cap H| \leq 2$. Let $h \in \langle \cup H_\alpha\rangle \cap H$. On the one hand, the action of $h$ on $V$ is $T$-linear, since $h \in H$. On the other hand, $h(u_1) = u_1$ and $h(u_2) = u_2 + \delta u_1$ for some $\delta \in T$. By our assumption above, either $h \in N_H(\langle u_2\rangle)$ and $\delta = 0$, or $h$ is an involution and $\delta = 1$. Thus we obtain the claim since $C_H(u_1) \cap C_H(u_2) = 1$.

Let $z$ be the generator of the group $\langle \cup H_\alpha\rangle \cap H$. This is a central element in $\langle \cup H_\alpha\rangle$. For every $g \in G$ let $\sigma_g \in \mathrm{Gal}(T|\mathbb{F}_q)$ denote the action of $g$ on $T$.

Let $g$ and $h$ be two elements of $\langle \cup H_\alpha\rangle$. Since $G/H$ is embedded into $\mathrm{Gal}(T|\mathbb{F}_q)$, we get $\sigma_g \neq \sigma_h$ unless $g = h$ or $g = hz$. Furthermore, a routine calculation shows that the subfields of $T$ fixed by $\sigma_g$ and $\sigma_h$ are the same if and only if $\langle g\rangle = \langle h\rangle$ or $\langle g\rangle = \langle hz\rangle$.

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 $\sigma_g$. Let $K_g = \{\alpha \in T \mid g \in H_\alpha\}$. The previous calculation shows that $K_g$ is an additive coset of the subfield fixed by $\sigma_g$, so $|K_g| = p^d$ for some $d \mid f = \log_q |T|$. Since for any $d \mid f$ there is a unique $p^d$-element subfield of $T$, we get $|K_g| \neq |K_h|$ unless the subfields fixed by $\sigma_g$ and $\sigma_h$ are the same. As we have seen, this means that $\langle g\rangle = \langle h\rangle$ or $\langle g\rangle = \langle hz\rangle$. Consequently, $|K_g| \neq |K_h|$ unless $K_g = K_h$ or $K_g = K_{hz}$. Hence we get

$$|\bigcup_{g\in \cup H_\alpha \setminus\{1\}} K_g| \leq 2 \sum_{d|f, d<f} q^d \leq 2\sum_{d<f} q^d < q^f = |T|.$$

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

Using Theorem 6.1, we can assume that $G \leq GL(l, T)$. As $l = \dim_T V < \dim_{\mathbb{F}_q}(V)$, we can use induction on the dimension of $V$, thus $b(G) \leq 2$.

By the last paragraph of Section 4, we need not consider Theorem 1.2 here.

Hence in the following we assume that $V$ is a direct sum of isomorphic absolutely irreducible $\mathbb{F}_q N$-modules for any $N \lhd G$.

## 7. Stabilizers of tensor product decompositions

Let $N \lhd G$ and let $V = V_1 \oplus \cdots \oplus V_k$ be a direct decomposition of $V$ into isomorphic absolutely irreducible $\mathbb{F}_q N$-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 [12, 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 $G/Z \simeq (G_1/Z) \times (G_2/Z)$, hence $G_1 \leq GL(n/k, q)$ and $G_2 \leq GL(k, q)$ are $p$-solvable irreducible linear groups. If $1 < k < n$, then by using induction for

$G_1 \leq GL(n/k,q)$ and $G_2 \leq GL(k,q)$ we get $b(G_1) \leq t(q)$ and $b(G_2) \leq t(q)$. Furthermore $b^*(G_1) \leq t(q)$ and $b^*(G_2) \leq t(q)$ by Corollary 3.3. Thus [14, Lemma 3.3 (ii)] gives us

$$b(G) \leq b(G_1 \otimes G_2) \leq b^*(G_1 \otimes G_2) \leq \max(b^*(G_1), b^*(G_2)) \leq t(q).$$

For the reduction of Theorem 1.2, by using induction on the dimension, we have

$$|G| \leq |G_1| \cdot |G_2| \leq 24^{-1/3} q^{(n/k)(d-1)} \cdot 24^{-1/3} q^{k(d-1)} \leq 24^{-1/3} |V|^{d-1}.$$

Thus, from now on we can assume that for every normal subgroup $N \lhd G$ either $N \leq Z$ or $V$ is absolutely irreducible as an $\mathbb{F}_q N$-module.

## 8. Groups of symplectic type

From now on assume that $N$ is a normal subgroup of $G$ containing $Z$ such that $N/Z$ is a minimal normal subgroup of $G/Z$. Then $N/Z$ is a direct product of isomorphic simple groups. In this section we examine the situation when $N/Z$ is an elementary Abelian group.

If $N$ is Abelian then it is central in $G$. So assume that $N$ is non-Abelian.

If $N/Z$ is elementary Abelian of rank at least 2, then $G$ is of symplectic type. Such groups were examined in [10, Section 5] (see also [10, Remark 5.20]) where it was proved that $b(G) \leq 2$ unless $q \in \{3, 4\}$, when $b(G) \leq 3$ holds.

For the reduction of Theorem 1.2, we need only examine the case $q = 3,\ n = 2^k$. For this we can use the fact that $G/N$ can be considered as a subgroup of the symplectic group $\mathrm{Sp}(2k, 2)$. By the theorem of Pálfy [16] and Wolf [20], we may assume that $G$ is a non-solvable (and 3-solvable) group. Thus we must have a composition factor of $G$ (and thus of $G/N$) isomorphic to a Suzuki group. Since the smallest Suzuki group $\mathrm{Suz}(8)$ has order larger than $|\mathrm{Sp}(4,2)|$, we must have $k \geq 3$. On the other hand, since the second largest Suzuki group $\mathrm{Suz}(32)$ has order larger than $|\mathrm{Sp}(6,2)|$ and since $\mathrm{Suz}(8)$ is not a section of $\mathrm{Sp}(6,2)$ (since 13 divides the order of the first group but not the order of the second), we see that $k \neq 3$. But for $k \geq 4$ we clearly have $|G| = |N||G/N| < 2^{2k^2+3k+3} < 24^{-1/3}|V|^{d-1}$, by use of the formula for the order of $\mathrm{Sp}(2k, 2)$.

## 9. Tensor product actions

Now let $N/Z$ be a direct product of $t \geq 2$ isomorphic non-Abelian simple groups. Then $N = L_1 \star L_2 \star \cdots \star L_t$ 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, $V \simeq V_1 \otimes V_2 \otimes \cdots \otimes V_t$ and $G$ permutes the factors of this tensor product. It follows that $G$ is embedded into the central wreath product $G_1 \wr_c S_t$. Clearly $G_1 \leq GL(V_1)$ is a $p$-solvable irreducible linear group. Thus $b(G_1) \leq t(q)$ and $b^*(G_1) \leq t(q)$ by induction on the dimension $m$ of $V_1$ and by Corollary 3.3.

First let $q \geq 5$. Then $t(q) = 2$. Thus $b(G) \leq 2$ follows from [10, Theorem 3.6] unless $(m,t) = (2,2)$. In case $(m,t) = (2,2)$, that is, $G \leq G_1 \wr_c S_2 \leq GL(4,q)$ for some $p$-solvable group $G_1 \leq GL(2,q)$ let $x_1, y_1 \in V_1$ be a basis of $V_1$ satisfying either $N_{G_1}(\langle x_1 \rangle) \subseteq N_{G_1}(\langle y_1 \rangle)$ or the property that every non-identity element of $C_{G_1}(x_1)$ takes $y_1$ to $y_1 + x_1$. (Such a basis exists by Theorem 3.1.) Now, it is easy to see that by choosing any $\alpha \in \mathbb{F}_q \setminus \{0,1\}$ we get that $x_1 \otimes x_1,\ y_1 \otimes (y_1 + \alpha x_1)$ is a base for $G_1 \wr_c S_2 \geq G$.

Now, let $q = 3$. Let $x_1, y_1, z_1 \in V_1$ be a strong base for $G_1$. Then the stabilizer of $\underbrace{x_1 \otimes x_1 \otimes \cdots \otimes x_1}_{t \text{ factors}} \in V$ is of the form $H = H_1 \wr_c S_t$, where $y_1, z_1 \in V_1$ is a strong base for $H_1 = N_{G_1}(x_1)$, so $b^*(H_1) \leq 2$. If $(m,t) \neq (2,2)$ then $b(H) \leq 2$ by [10, Theorem 3.6], which results in $b(G) \leq 3$. Finally, let $(m,t) = (2,2)$. By choosing a basis $x_1, y_1 \in V_1$, it is easy to see that $x_1 \otimes x_1, y_1 \otimes y_1, x_1 \otimes y_1 \in V$ is a base for $GL(V_1) \wr_c S_2 \geq G$.

As for the order of $G$ notice that $G \leq G_1 \wr_c S$ where $S \leq S_t$ is a 3-solvable group. Thus by induction and by [15, Corollary 1.5] we have

$$|G| \leq |G_1|^t |S| \leq 24^{-t/3} |V_1|^{(d-1)t} 24^{(t-1)/3} = 24^{-1/3} |V|^{d-1}.$$

## 10. Almost quasisimple groups

Finally, let $Z \leq N \lhd G$ be such that $N/Z$ is a non-Abelian simple group. Let $N_1 = [N,N] \lhd G$ and let $V_1$ be an irreducible $\mathbb{F}_p N_1$-submodule of $V$ and $G_1 = \{g \in G \,|\, g(V_1) = V_1\}$ be the stabilizer of $V_1$. By using the same argument as in the last paragraph of [10, Page 29] we get that $G_1$ is included in $GL(V_1)$ and we have a chain of subgroups $N_1 \lhd G_1 \leq GL(V_1)$ where $G_1$ is $p$-solvable, $N_1$ is quasisimple and $V_1$ is irreducible as an $\mathbb{F}_p N_1$-module.

Suppose that $b(G_1) \leq 2$ in the action of $G_1$ on $V_1$, that is, there exist $x, y \in V_1 \leq V$ such that $C_{G_1}(x) \cap C_{G_1}(y) = 1$. For any element $g \in G$ with $g(x) = x$ we have that $N_1 x = \{nx \,|\, n \in N_1\}$ is a $g$-invariant subset. As the $\mathbb{F}_p$-subspace generated by $N_1 x$ is exactly $V_1$, we get that $g \in G_1$. This proves that $C_G(x) \cap C_G(y) = C_{G_1}(x) \cap C_{G_1}(y) = 1$. Thus $b(G) \leq 2$.

Hence if we manage to show that $b(G_1) \leq 2$ then we are finished with the proofs of both Theorems 1.1 and 1.2.

So assume that $G = G_1$ and $V = V_1$. Moreover, by the previous sections, we have that $q = p$. Also $N = N_1$. To summarize, $G \leq GL(V)$ is a group having a quasisimple irreducible normal subgroup $N$ containing $Z$.

We claim that $G/Z$ is almost simple. For this it is sufficient to see that $N/Z$ is the unique minimal normal subgroup of $G/Z$. For let $M/Z$ be another minimal normal subgroup of $G/Z$. By Section 8, we may assume that $M/Z$ is non-Abelian. Furthermore the group $MN$ is a central product and so $[M,N] = 1$. But this is impossible since the centralizer of $N$ in $G$ must be Abelian.

**Lemma 10.1.** *If $N$ has a regular orbit on $V$ then $b(G) \leq 2$.*

*Proof.* Since $N$ is normal in $G$ a regular $N$-orbit $\Delta$ containing a given vector $v$ is a block of imprimitivity inside the $G$-orbit containing $v$. Hence the group $C_G(v)N$ is transitive on $\Delta$ and $N$ is regular on $\Delta$. Thus for every $h \in C_G(v)$ the number

$|\mathrm{fix}(h)|$ of fixed points of $h$ on $\Delta$ is $|C_N(h)|$. To prove that $G$ has a base of size at most 2 on $V$, it is sufficient to see that there exists a vector $w$ in $\Delta$ that is not fixed by any non-trivial element of $C_G(v)$.

First notice that if $N/Z(N)$ is isomorphic to the non-Abelian finite simple group $S$ then $|C_G(v)| \leq |\mathrm{Out}(S)| < m(S)$ where $m(S)$ is the minimal index of a proper subgroup of $S$. This latter inequality follows from [1, Lemma 2.7 (i)].

But

$$\sum |\mathrm{fix}(h)| = \sum |C_N(h)| < |C_G(v)| \cdot \frac{|N|}{m(S)} < |N|$$

where the sums are over all non-identity elements $h$ in $C_G(v)$. This completes the proof of the lemma. □

By Lemma 10.1, in the following we may assume that $N$ does not have a regular orbit on $V$. Our final theorem finishes the proofs of Theorems 1.1 and 1.2.

**Theorem 10.2.** *Under the current assumptions $G$ is a $p'$-group and $b(G) \leq 2$.*

*Proof.* By using Goodwin's theorem [9, Theorem 1], Köhler and Pahlings [13, Theorem 2.2] gave a complete list of (irreducible) quasisimple $p'$-groups $N$ such that $N$ does not have a regular orbit on $V$. In all these exceptional cases, when $N/Z$ is simple, $|\mathrm{Out}(N/Z)|$ is divisible by no prime larger than 3 while $p$ is always at least 5. So $G$ itself is a $p'$-group. But then $G$ admits a base of size 2 on $V$ by [10, Theorem 4.4]. □

## References


[1] Aschbacher, M.; Guralnick, R. M. On Abelian quotients of primitive groups. *Proc. Amer. Math. Soc.* **107** (1989), 89–95.

[2] Cossey, J. P.; Halasi, Z.; Maróti, A.; Nguyen, H. N. On a conjecture of Gluck, to appear in *Math. Z.*

[3] Dolfi, S. Orbits of permutation groups on the power set. *Arch. Math.* **75** (2000), 321–327.

[4] Dolfi, S. Intersections of odd order Hall subgroups. *Bull. London Math. Soc.* **37** (2005) 61–66.

[5] Dolfi, S. Large orbits in coprime actions of solvable groups. *Trans. Amer. Math. Soc.* **360** (2008), 135–152.

[6] Dolfi, S.; Jabara, E. Large character degrees of solvable groups with Abelian Sylow 2-subgroups. *J. Algebra* **313** (2007), 687–694.

[7] The GAP Group, GAP – Groups, Algorithms, and Programming, Version 4.6.3; 2013. (http://www.gap-system.org)

[8] Gluck D.; Magaard, K. Base sizes and regular orbits for coprime affine permutation groups. *J. London Math. Soc.* (2) **58** (1998), 603–618.

[9] Goodwin, D. P. M. Regular orbits of linear groups with an application to the $k(GV)$-problem, I,II. *J. Algebra* **227** (2000), 395–432 and 433–473.

[10] Halasi, Z.; Podoski, K. Every coprime linear group admits a base of size two, to appear in *Trans. Amer. Math. Soc.*

[11] Huppert, B.; Blackburn, N. Finite groups. III. Grundlehren der Mathematischen Wissenschaften, 243. Springer-Verlag, Berlin-New York, 1982.

[12] Kleidman, P.; Liebeck, M. The subgroup structure of the finite classical groups. London Mathematical Society Lecture Note Series, 129. Cambridge University Press, Cambridge, 1990.

[13] Köhler, C.; Pahlings, H. 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.

[14] Liebeck, M. W.; Shalev, A. Bases of primitive linear groups. *J. Algebra* **252** (2002), 95–113.

[15] Maróti, A. On the orders of primitive groups. *J. Algebra* **258** (2002), 631–640.

[16] Pálfy, P. P. A polynomial bound for the orders of primitive solvable groups. *J. Algebra* **77** (1982), 127–137.
[17] Pálfy, P. P. Bounds for linear groups of odd order. Proceedings of the Second International Group Theory Conference (Bressanone, 1989). Rend. Circ. Mat. Palermo (2) Suppl. No. 23 (1990), 253–263.
[18] Seress, Á. The minimal base size of primitive solvable permutation groups. *J. London Math. Soc.* **53** (1996) 243–255.
[19] Vdovin, E. P. Regular orbits of solvable linear $p'$-groups. *Sib. Élektron. Mat. Izv.* **4** (2007), 345–360.
[20] Wolf, T. R. Solvable and nilpotent subgroups of $GL(n, q^m)$. *Canad. J. Math.* **34** (1982), 1097–1111.
[21] Wolf, T. R. Large orbits of supersolvable linear groups. *J. Algebra* **215** (1999), 235–247.
[22] Yang, Y. Large character degrees of solvable $3'$-groups. *Proc. Amer. Math. Soc.* **139** (2011), 3171–3173.

Department of Algebra and Number Theory, Institute of Mathematics, University of Debrecen, 4010, Debrecen, Pf. 12, Hungary

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

Fachbereich Mathematik, Technische Universität Kaiserslautern, Postfach 3049, 67653 Kaiserslautern, Germany and Alfréd Rényi Institute of Mathematics, Reáltanoda utca 13-15, H-1053, Budapest, Hungary

*E-mail address*: `maroti@mathematik.uni-kl.de and maroti.attila@renyi.mta.hu`