The number of homomorphisms from a finite group to a general linear group

Martin W. Liebeck
Department of Mathematics
Imperial College
London SW7 2BZ
England
m.liebeck@ic.ac.uk

Aner Shalev
Institute of Mathematics
Hebrew University
Jerusalem 91904
Israel
shalev@math.huji.ac.il

Abstract

Given a finite group A we estimate the number of homomorphisms from A to $GL_n(q)$, where q is a prime power coprime to $|A|$.

1 Introduction

Let A be a finite group. In [5] Müller studies the number of homomorphisms from A to the symmetric group S_n, deriving a precise asymptotic expansion as n tends to infinity. In this note we study the linear version of this problem, where the symmetric group S_n is replaced by a finite general linear group $GL_n(q)$.

Preliminary results of this type have already been obtained. The case where A is of order 2 or 3 can be found in [2, 4.1] (in this case one is of course essentially counting the number of elements of order 2 or 3 in the general linear group). More generally, the case where A has prime order is handled in [3, Lemma 1]. These results deal with both the modular case (where q and $|A|$ are not coprime) and the non-modular case. However, for more general groups A the behaviour of $|\mathrm{Hom}(A, GL_n(q))|$ seems to be very different in the modular and non-modular cases (see section 3 below), and we assume here that q and $|A|$ are coprime. We derive lower and upper bounds for $|\mathrm{Hom}(A, GL_n(q))|$ which are of roughly the same order of magnitude when n is large, but we do not provide a precise asymptotic expansion. Note that in [1], $|\mathrm{Hom}(A, GL_n(q))|$ is studied using generating functions, but bounds for its order of magnitude are not provided.

The second author acknowledges the support of an EPSRC Visiting Fellowship at Imperial College London, and a grant from the Israel Science Foundation

1991 *Mathematics Subject Classification:* 20D06, 20E05, 20E26, 20P05.

Our main result is as follows.

Theorem *Let A be a finite group of order a, p a prime not dividing a, q a power of p and n a positive integer. Then there is an absolute constant c, and a number $d = d(a)$ depending only on a, such that*

$$cq^{-a^2}|GL_n(q)|^{1-a^{-1}} < |\mathrm{Hom}(A, GL_n(q))| < d|GL_n(q)|^{1-a^{-1}}.$$

In fact our proof produces a somewhat better lower bound as follows. Write $n = ka + r$ where k is an integer and $0 \leq r < a$. Then we show $|\mathrm{Hom}(A, GL_n(q))| > cq^{-b}|GL_n(q)|^{1-a^{-1}}$, where $b = r^2(1 - a^{-1})$; in particular, if n is divisible by a we obtain

$$c|GL_n(q)|^{1-a^{-1}} < |\mathrm{Hom}(A, GL_n(q))| < d(a)|GL_n(q)|^{1-a^{-1}}.$$

The assumption in the Theorem that p does not divide a, and the dependence of the constant d on a, are essential, as we show with various examples in Section 3.

Our result can also be viewed in the context of representation varieties (see Lubotzky-Magid [4]). In fact the strategy of our proof is first to study the algebraic variety of homomorphisms from A to $GL_n(K)$ where K is the algebraic closure of $\mathbb{F}_q$, and then to pass to finite fields by taking fixed points of a Frobenius morphism. A result of Richardson [6] which implies that the $GL_n(K)$-orbits on $\mathrm{Hom}(A, GL_n(K))$ are closed (in the non-modular case) plays a key role in the proof.

It is certainly possible to prove the theorem staying entirely within the realm of the representation theory of finite groups. However, we prefer our algebraic group approach, firstly because we find it rather elementary and conceptual, and secondly because the method may well generalise to other classical groups.

2 Proof of the Theorem

We shall use throughout the elementary observation that there is an absolute constant $\beta > 0$ such that $\beta q^{n^2} < |GL_n(q)| < q^{n^2}$: indeed, $\beta = \prod_{i=1}^{\infty}(1 - 2^{-i})$ fits the bill.

We begin by establishing the lower bound for $|\mathrm{Hom}(A, GL_n(q))|$ in the Theorem. Write $n = ka + r$ with $0 \leq r < a$, and let $F = \mathbb{F}_q$. Define the FA-module $V = M \oplus I$, where M is a free FA-module of rank k and I is a trivial module of dimension r. Let $\phi : A \to GL_n(q)$ be the corresponding

representation of A. Then

$$\begin{aligned}\dim_F(\mathrm{Hom}_{FA}(V,V)) &= \dim_F(\mathrm{Hom}_{FA}(M,M)) + 2\dim_F(\mathrm{Hom}_{FA}(M,I)) + \\ &\quad \dim_F(\mathrm{Hom}_{FA}(I,I)) \\ &= ak^2 + 2kr + r^2 = n^2a^{-1} + r^2(1-a^{-1}).\end{aligned}$$

Hence

$$|C_{GL_n(q)}(\phi(A))| \leq |\mathrm{Hom}_{FA}(V,V))| = q^{n^2a^{-1}+r^2(1-a^{-1})}.$$

For $g \in GL_n(q)$, define $\phi^g \in \mathrm{Hom}(A, GL_n(q))$ to send $x \to \phi(x)^g$ $(x \in A)$. Then the number of distinct such conjugates of ϕ is

$$|GL_n(q) : C_{GL_n(q)}(\phi(A))| > c_1 q^{n^2-(n^2a^{-1}+r^2(1-a^{-1}))} = c_1 q^{(n^2-r^2)(1-a^{-1})}$$

Hence $|\mathrm{Hom}(A, GL_n(q))| > c_1 q^{(n^2-r^2)(1-a^{-1})}$, giving the lower bound in the Theorem.

Now we prove the upper bound in the Theorem. Let $K = \bar{\mathbb{F}}_q$, the algebraic closure of $\mathbb{F}_q$, and let σ be the Frobenius morphism of $G = GL_n(K)$ sending $(a_{ij}) \to (a_{ij}^q)$, so that the fixed point group $G_\sigma = GL_n(q)$.

Consider the variety $X = \mathrm{Hom}(A, G)$. Then σ acts on X: for $\phi \in X$ and $x \in A$ we define $\phi^\sigma(x) = \phi(x)^\sigma$. The fixed point set X_σ is $\mathrm{Hom}(A, GL_n(q))$.

Also G acts on X via $\phi^g(x) = \phi(x)^g$ $(\phi \in X, g \in G, x \in A)$. Since by hypothesis p does not divide $|A|$, all $\phi \in X$ are completely reducible representations. Hence [6, Section 16] shows that the G-orbits on X are all closed, and are the irreducible components of the variety X.

We aim to find an upper bound for the size of the fixed point set X_σ. For this we need only consider σ-invariant orbits of G on X.

Let $\rho_1, \ldots, \rho_m$ be a full set of inequivalent irreducible representations of A over K, and let d_i be the degree of ρ_i. The G-orbits on X correspond bijectively in a natural way with m-tuples of non-negative integers $(n_1, \ldots, n_m)$ such that $\sum n_i d_i = n$.

Fix a σ-invariant G-orbit $Y \subseteq X$, with corresponding m-tuple $(n_1, \ldots, n_m)$. For $\phi \in Y$, the stabilizer $\mathrm{stab}_G(\phi) = C_G(\phi(A))$. Since ϕ is a completely reducible representation, Schur's Lemma implies that $C_G(\phi(A)) = \prod_1^m GL_{n_i}(K)$, a closed connected subgroup of G. In particular, $\dim Y = n^2 - \sum_1^m n_i^2$. Now Lang's theorem (see [7, 2.2,2.8]) shows that G_σ is transitive on Y_σ. Take $\phi \in Y_\sigma$. Now $G_\sigma = GL_n(q)$ has order less than $q^{\dim G}$, while $C_G(\phi(A))_\sigma$ is a product of GL_{n_i}'s over extensions of $\mathbb{F}_q$ and has order at least $b(a)q^{\sum n_i^2}$, where $b(a)$ depends only on a. It follows that

$$|Y_\sigma| = |G_\sigma : C_G(\phi(A))_\sigma| < c(a)q^{\dim Y}.$$

Define $t = \frac{n}{a}$, and set $r_i = n_i - td_i$. Then

$$n = \sum n_i d_i = t \sum d_i^2 + \sum r_i d_i = ta + \sum r_i d_i = n + \sum r_i d_i,$$

and so $\sum r_i d_i = 0$. Hence

$$\sum_1^m n_i^2 = \sum (td_i + r_i)^2 = t^2 \sum d_i^2 + \sum r_i^2 + 2t \sum d_i r_i = t^2 a + \sum r_i^2 = n^2 a^{-1} + f,$$

where $f = \sum r_i^2 \geq 0$. We deduce that

$$|Y_\sigma| < c(a) q^{n^2(1-a^{-1})-f}.$$

Note that each r_i is an integer multiple of a^{-1}, so f is an integer multiple of a^{-2}. Given such a non-negative rational $f = ha^{-2}$, the number of m-tuples $(r_1, \ldots, r_m)$ satisfying $\sum r_i^2 = f$ is at most $(2\sqrt{h}+1)^m$. This is an upper bound for the number of σ-invariant orbits Y for which $f = ha^{-2}$. Summing over all possible h, we obtain

$$|X_\sigma| < c(a) \sum_{h \geq 0} (2\sqrt{h}+1)^m q^{n^2(1-a^{-1})-ha^{-2}}.$$

The sum $\sum_{h\geq 0}(2\sqrt{h}+1)^m q^{-ha^{-2}}$ is finite and bounded by a function of a. Therefore

$$|X_\sigma| < c'(a) q^{n^2(1-a^{-1})} < d(a) |GL_n(q)|^{1-a^{-1}}.$$

Since $X_\sigma = \mathrm{Hom}(A, GL_n(q))$, this gives the upper bound in the Theorem.

3 Examples

We present some examples showing that the assumption in the Theorem that p does not divide a, and the dependence of the constant d on a, are essential.

Example 1 Let p be a prime and q a power of p. Let $A = (C_p)^s$, let $n = 2m$ be even, and define

$$E = \{ \begin{pmatrix} I_m & X \\ 0 & I_m \end{pmatrix} : X \text{ is } m \times m \text{ over } \mathbb{F}_q \} < GL_n(q).$$

Then E is elementary abelian of order q^{m^2}, so

$$|\mathrm{Hom}(A, GL_n(q))| \geq q^{m^2 s},$$

which for large s is greater than the upper bound in the Theorem, and indeed greater than any fixed power of $|GL_n(q)|$.

Example 2 Let $A = C_a$ where a divides $q-1$. If $n = ka$ with k a positive integer, it is easy to see that the number of elements of order a in $GL_n(q)$ is at least

$$cq^{n^2(1-a^{-1})}(1 + a(a-1)q^{-2}).$$

Indeed, the first term comes from taking all $n_i = k$ (defining n_i as in the above proof), and the second by taking $n_i = k+1, n_j = k-1$ and the rest equal to k, over all possible ordered pairs (i, j). Consequently

$$|\mathrm{Hom}(A, GL_n(q))| > c(1 + a(a-1)q^{-2})|GL_n(q)|^{1-a^{-1}}.$$

For q fixed and a large this shows the necessity for the dependence of d on a in the Theorem.

References

[1] N. Chigira, Y. Takegahara and T. Yoshida, On the number of homomorphisms from a finite group to a general linear group, *J. Algebra* **232** (2000), 236–254.

[2] M.W. Liebeck and A. Shalev, Classical groups, probabilistic methods, and the $(2,3)$-generation problem, *Annals of Math.* **144** (1996), 77–125.

[3] M.W. Liebeck and A. Shalev, Random (r,s)-generation of finite classical groups, *Bull. London Math. Soc.* **34** (2002), 185-188.

[4] A. Lubotzky and A.R. Magid, Varieties of representations of finitely generated groups, *Mem. Amer. Math. Soc.* **58** (1985), no. 336.

[5] T. Müller, Finite group actions and asymptotic expansion of $e^{P(z)}$, *Combinatorica* **17** (1997), 523–554.

[6] R. Richardson, Conjugacy classes of n-tuples in Lie algebras and algebraic groups, *Duke Math. J.* **57** (1988), no. 1, 1–35.

[7] T.A. Springer and R. Steinberg, Conjugacy classes, in: *Seminar on algebraic groups and related topics* (ed. A. Borel et al.), Lecture Notes in Math. 131, Springer, Berlin, 1970, pp. 168-266.