UNIVERSITY of York

This is a repository copy of *Asymptotic Bounds for the Size of Hom(A,GL_n(q))*.

White Rose Research Online URL for this paper:
https://eprints.whiterose.ac.uk/113941/

Version: Accepted Version

Article:
Bate, Michael orcid.org/0000-0002-6513-2405 and Gullon, Alec (2018) Asymptotic Bounds for the Size of Hom(A,GL_n(q)). Glasgow Mathematical Journal. pp. 51-61. ISSN 1469-509X

https://doi.org/10.1017/S0017089516000562

Reuse
Items deposited in White Rose Research Online are protected by copyright, with all rights reserved unless indicated otherwise. They may be downloaded and/or printed for private study, or other acts as permitted by national copyright laws. The publisher or other rights holders may allow further reproduction and re-use of the full text version. This is indicated by the licence information on the White Rose Research Online record for the item.

Takedown
If you consider content in White Rose Research Online to be in breach of UK law, please notify us by emailing eprints@whiterose.ac.uk including the URL of the record and the reason for the withdrawal request.

White Rose university consortium
Universities of Leeds, Sheffield & York

eprints@whiterose.ac.uk
https://eprints.whiterose.ac.uk/

ASYMPTOTIC BOUNDS FOR THE SIZE OF $\mathrm{Hom}(A, \mathrm{GL}_n(q))$.

MICHAEL BATE AND ALEC GULLON

Abstract. Fix an arbitrary finite group A of order a, and let $X(n,q)$ denote the set of homomorphisms from A to the finite general linear group $\mathrm{GL}_n(q)$. The size of $X(n,q)$ is a polynomial in q. In this note it is shown that generically this polynomial has degree $n^2(1-a^{-1})-\epsilon_r$ and leading coefficient m_r, where ϵ_r and m_r are constants depending only on $r := n \mod a$. We also present an algorithm for explicitly determining these constants.

1. Introduction

Let A be a finite group of order a and let $X(n,q) = \mathrm{Hom}(A, \mathrm{GL}_n(q))$ denote the set of all homomorphisms from A to the general linear group of $n \times n$ invertible matrices with entries in the finite field $\mathbb{F}_q$. Suppose that $\mathbb{F}_q$ is a splitting field for A. In [5], Liebeck and Shalev provide upper and lower bounds for the size of this set, which is a polynomial in q [2, Prop. 4.1]; see also [1]. The bound presented in [5, Theorem] has the following form:

$$cq^{(n^2-r^2)(1-a^{-1})} \leq |X(n,q)| \leq dq^{n^2(1-a^{-1})},$$

where c is an absolute constant, d is a constant depending only on a, and r is the value of n modulo a. Note that, as is pointed out in [5] and [1], there is an absolute constant $\beta > 0$ such that $\beta q^{n^2} \leq |\mathrm{GL}_n(q)| \leq q^{n^2}$ for all n and q, so these bounds can be rewritten in terms of the order of $\mathrm{GL}_n(q)$. The aim of this note is to show that there exists N such that for all $n \geq N$ the leading term of the polynomial $|X(n,q)|$ has the form

$$m_r q^{n^2(1-a^{-1})-\epsilon_r},$$

where (given a fixed group A) m_r and ϵ_r are constants only depending on r, and $N = a(a-1)$ will definitely suffice. In particular, this leading coefficient and degree are independent of q. We also present an algorithm for explicitly determining the values of m_r, ϵ_r and N for any choice of A. The input needed for the algorithm is the degrees of the irreducible representations for A over a splitting field for A.

The paper is laid out as follows. We begin in Section 2 by setting up some basic notation and recalling some of the analysis from [5] and [1], before moving on to the main results in Section 3. After giving some examples to illustrate various points of the paper in Section 4, in the final section of the paper we indicate how to relax some of the assumptions in force for the rest of the paper, and also make some further remarks.

2. Preliminaries

Throughout, A denotes a finite group with a elements. We use q to denote the order of a finite field $\mathbb{F}_q$, so $q = p^d$ for some prime p and positive integer d. Our standing assumption

2010 *Mathematics Subject Classification.* 20G40, 20C15.

Key words and phrases. Finite group; counting homomorphisms; representation variety.

on q for most of this note (except in Section 5) is that $\mathbb{F}_q$ is a splitting field for A, i.e., the characteristic p of the field $\mathbb{F}_q$ does not divide a and all irreducible $\mathbb{F}_qA$-modules are absolutely irreducible. By Schur's Lemma, given a simple $\mathbb{F}_qA$-module M, we have $\mathrm{End}_{\mathbb{F}_qA-\mathrm{mod}}(M) \simeq \mathbb{F}_q$.

For an n-dimensional $\mathbb{F}_q$-vector space V, we have the finite general linear group $\mathrm{GL}(V)$ which we freely identify with $\mathrm{GL}_n(q)$, the group of invertible $n \times n$ matrices with entries in $\mathbb{F}_q$, when it is convenient to do so. We let $X(n,q) = \mathrm{Hom}(A, \mathrm{GL}_n(q))$ denote the set of homomorphisms from A to $\mathrm{GL}_n(q)$ for each choice of n and q, and note that $\mathrm{GL}_n(q)$ acts on $X(n,q)$ by conjugation: given $\rho : A \to \mathrm{GL}_n(q)$ and $g \in \mathrm{GL}_n(q)$, set $(g \cdot \rho)(a) = g\rho(a)g^{-1}$ for all $a \in A$. This breaks the set $X(n,q)$ up into $\mathrm{GL}_n(q)$-orbits, and one key part of the analysis in [5] and [1] is to bound the size of each of these orbits. This involves some basic representation theory, which we now recap.

Let $(M_1, \ldots, M_s)$ be a complete ordered tuple of pairwise non-isomorphic irreducible (hence absolutely irreducible by our assumptions on the field) $\mathbb{F}_qA$-modules, and let $d_i = \dim(M_i)$ for each i. Choose the labelling so that M_1 is the trivial module. The degrees d_i are the same for any splitting field for A, and $a = \sum_{i=1}^{s} d_i^2$. Given any $\mathbb{F}_qA$-module V, we have an isomorphism

$$V \simeq n_1M_1 \oplus \cdots \oplus n_sM_s,$$

where n_iM_i denotes the direct sum of the module M_i with itself n_i times (we allow $n_i = 0$ here). For a given $\mathbb{F}_qA$-module V, we therefore have an ordered s-tuple $(n_1, \ldots, n_s)$ of non-negative integers and two $\mathbb{F}_qA$-modules are isomorphic if and only if they have the same ordered s-tuple attached. Moreover, if we restrict attention to n-dimensional modules for some fixed n, then the relevant s-tuples $(n_1, \ldots, n_s)$ for which $\sum_{i=1}^{s} n_id_i = n$ also parametrise the $\mathrm{GL}_n(q)$-orbits in $X(n,q)$. It follows from the analysis in [5] and [1] that, given a tuple $(n_1, \ldots, n_s)$, the stabilizer associated to the corresponding orbit in $X(n,q)$ is isomorphic to a product $\prod_{i=1}^{s} \mathrm{GL}_{n_i}(q)$, which allows us to write down the size of the orbit by the Orbit-Stabilizer Theorem. The key to the approach presented in this note is to give a better estimate of the largest possible size for such an orbit, and to show that such a size is attained, which improves on the upper and lower bounds presented in [5].

3. Results

Keep the notation from the previous section, and remember our standing assumption that $\mathbb{F}_q$ is a splitting field for A. Before stating and proving the main technical results needed for our algorithm, we introduce some more terminology. Let $n \in \mathbb{N}$. We say that an ordered tuple $(n_1, \ldots, n_s)$ of integers (not necessarily non-negative) is *admissible for* n if $\sum_{i=1}^{s} n_id_i = n$; if the context is clear, then we simply say the tuple is admissible. We call such an admissible tuple *eligible* if, in addition, $n_i \geq 0$ for all i. Finally, we call a tuple $(n_1, \ldots, n_s)$ which is admissible for $n \in \mathbb{N}$ a *minimal tuple for* n if $\sum_{i=1}^{s} n_i^2$ is minimal amongst all admissible tuples for n.

Lemma 3.1. *Fix $n \in \mathbb{N}$. Then:*

(i) *the parametrisation of the orbits in $X(n,q)$ by eligible tuples is independent of q;*
(ii) *for each eligible tuple $\mathbf{t} = (n_1, \ldots, n_s)$, there is a polynomial $f_{\mathbf{t}}(x) \in \mathbb{Z}[x]$ such that the size of the corresponding orbit in $X(n,q)$ is $f_{\mathbf{t}}(q)$.*
(iii) *the polynomials of maximal degree from (ii) are precisely those corresponding to minimal tuples.*

Proof. Part (i) follows from the fact that the dimensions and number of isomorphism classes of absolutely irreducible $\mathbb{F}_q A$-modules over a splitting field are independent of that field. Then (ii) follows because the shape of the stabilizer of a given orbit, as given at the end of the previous section, is independent of q. Specifically, given any eligible tuple $(n_1, \ldots, n_s)$, the size of the associated orbit in $X(n, q)$ is $|\operatorname{GL}_n(q)| / \prod_{i=1}^s |\operatorname{GL}_{n_i}(q)|$, which is a polynomial in q [2, Prop. 4.1] with leading term $q^{n^2 - \sum_{i=1}^s n_i^2}$. Therefore, the largest degree amongst all these polynomials is attained by those polynomials corresponding to tuples for which $\sum_{i=1}^s n_i^2$ is minimal. These are precisely the polynomials corresponding to minimal eligible tuples, which proves (iii). □

Lemma 3.2. *Given $n \in \mathbb{N}$, there are finitely many minimal tuples for n.*

Proof. Since $d_1 = 1$, the tuple $(n, 0, 0, \ldots, 0)$ is admissible for n, and hence for a minimal tuple $(n_1, \ldots, n_s)$ we have $\sum_{i=1}^s n_i^2 \leq n^2$. In particular, for each i we have $-n \leq n_i \leq n$. This gives rise to finitely many tuples, and all the minimal tuples lie amongst these. □

The above lemma shows that for each n we have finitely many minimal tuples to worry about. In fact, we can do much better than that, as the following results show.

Lemma 3.3. *Given $n \in \mathbb{N}$, write $n = ka + r$ where $k \in \mathbb{N} \cup \{0\}$ and $0 \leq r < a$.*

(i) *Suppose $(r_1, \ldots, r_s)$ is a minimal tuple for r. Then $(kd_1 + r_1, \ldots, kd_s + r_s)$ is a minimal tuple for n.*
(ii) *Suppose $(n_1, \ldots, n_s)$ is a minimal tuple for n. Then $(n_1 - kd_1, \ldots, n_s - kd_s)$ is a minimal tuple for r.*

Hence minimal tuples for n are in 1-1 correspondence with minimal tuples for r.

Proof. First note that if $(r_1, \ldots, r_s)$ is an admissible tuple for r then $\sum_{i=1}^s r_i d_i = r$, so

$$\sum_{i=1}^s (kd_i + r_i) d_i = k \sum_{i=1}^s d_i^2 + \sum_{i=1}^s r_i d_i = ka + r = n,$$

and hence $(kd_1 + r_1, \ldots, kd_s + r_s)$ is admissible for n. Conversely, if $(n_1, \ldots, n_r)$ is admissible for n, then

$$\sum_{i=1}^s (n_i - kd_i) d_i = \sum_{i=1}^s n_i d_i - k \sum_{i=1}^s d_i^2 = n - ka = r,$$

so $(n_1 - kd_1, \ldots, n_s - kd_s)$ is admissible for r.

Now suppose $(r_1, \dots, r_s)$ is minimal for r and $(n_1, \dots, n_s)$ is minimal for n. Since $(r_1, \dots, r_s)$ is minimal for r and $(n_1 - kd_1, \dots, n_s - kd_s)$ is admissible for r, we have

$$\begin{aligned}
\sum_{i=1}^{s}(kd_i + r_i)^2 &= k^2 \sum_{i=1}^{s} d_i^2 + 2k \sum_{i=1}^{s} r_i d_i + \sum_{i=1}^{s} r_i^2 \\
&= k^2 a + 2kr + \sum_{i=1}^{s} r_i^2 \\
&\leq k^2 a + 2kr + \sum_{i=1}^{s}(n_i - kd_i)^2 \\
&= k^2 a + 2kr + \sum_{i=1}^{s} n_i^2 - 2k \sum_{i=1}^{s} n_i d_i + k^2 \sum_{i=1}^{s} d_i^2 \\
&= \sum_{i=1}^{s} n_i^2 + 2k^2 a + 2kr - 2kn \\
&= \sum_{i=1}^{s} n_i^2.
\end{aligned}$$

But $(n_1, \dots, n_r)$ is minimal for n, so we must actually have equality here and hence $(kd_1 + r_1, \dots, kd_s + r_s)$ is also minimal for n. Using this equality, we now also have

$$\begin{aligned}
\sum_{i=1}^{s}(n_i - kd_i)^2 &= \sum_{i=1}^{s} n_i^2 - 2k \sum_{i=1}^{s} n_i d_i + k^2 \sum_{i=1}^{s} d_i^2 \\
&= \sum_{i=1}^{s}(kd_i + r_i)^2 - 2kn + k^2 a \\
&= 2k^2 a + 2kr + \sum_{i=1}^{s} r_i^2 - 2k(ka + r) \\
&= \sum_{i=1}^{s} r_i^2,
\end{aligned}$$

so $(n_1 - kd_1, \dots, n_s - kd_s)$ is a minimal tuple for r. □

Remark 3.4. Lemma 3.3 is really at the heart of this note. It shows that, despite the fact that the whole set $X(n, q)$ gets more and more complicated as n grows, we can still exert some control over the orbits which are largest in the sense of Lemma 3.1(iii). One cannot hope for this to be true for smaller orbits, because as n grows, so does the number of eligible tuples and hence the total number of orbits.

Lemma 3.5. *There exists $N \in \mathbb{N}$ such that for all $n \geq N$, all minimal tuples for n are eligible and the number of minimal tuples only depends on the value of n modulo a.*

Proof. For any $n \in \mathbb{N}$, the number of minimal tuples for n is the same as the number of minimal tuples for r, where $n = ka + r$ with $k \in \mathbb{N} \cup \{0\}$ and $0 \leq r < a$, by Lemma 3.3, so this number only depends on the value of n modulo a. Moreover, the minimal tuples for n

all have the form $(kd_1+r_1,\dots,kd_s+r_s)$ where $(r_1,\dots,r_s)$ is a minimal tuple for r, again by Lemma 3.3. There are finitely many values r_i as r runs over all integers between 0 and $a-1$ by the argument in the proof of Lemma 3.2, and we just need to choose N large enough so that for all $n \geq N$, all possible values $kd_i + r_i \geq 0$, which can clearly be done. After this point, all the minimal tuples are also eligible. □

Remark 3.6. By the argument in the proof of Lemma 3.2, if $(r_1,\dots,r_s)$ is a minimal tuple for $0 \leq r < a$, the minimal possible value for any r_i is $-r$. Since each $d_i \geq 1$ this means that $kd_i+r_i \geq 0$ as long as $k > a-1$ for any choice of $0 \leq r < a$, so we could choose $N = a(a-1)$ in Lemma 3.5 if we wanted a concrete bound. However, in practice, as we shall see, the best value for N is often much less than this.

Remark 3.7. When $n = ka$ is a multiple of a, the tuple $(kd_1,\dots,kd_r)$ is the unique minimal eligible tuple for n. This is because this tuple gives a global minimum for the value $\sum_{i=1}^s x_i^2$ amongst all tuples of real numbers $(x_1,\dots,x_s)$ satisfying the constraint $\sum_{i=1}^s x_i d_i = n$, as can be verified using some basic calculus.

Proposition 3.8. *Suppose $0 \leq r < a$. Let m_r be the number of minimal tuples for r, and let $(r_1,\dots,r_s)$ be one of the minimal tuples for r. Let $\epsilon_r = \sum_{i=1}^s r_i^2 - r^2a^{-1}$. Given $n \in \mathbb{N}$ with $n \geq N$, where N is as in Lemma 3.5, write $n = ka + r$, where $k \in \mathbb{Z}$ and $0 \leq r < a$. Then*

(i) *$\epsilon_r \geq 0$ (with equality if and only if $r = 0$);*
(ii) *there exists a polynomial $f_n(x) \in \mathbb{Z}[x]$, independent of q, whose leading term is $m_r x^{n^2(1-a^{-1})-\epsilon_r}$ such that $|X(n,q)| = f_n(q)$.*

Proof. (i). The global minimum value for $\sum_{i=1}^s x_i^2$ amongst all real s-tuples $(x_1,\dots,x_s)$ satisfying $\sum_{i=1}^s x_i d_i = r$ is given by the tuple $(a^{-1}rd_1,\dots,a^{-1}rd_s)$, and hence $\sum_{i=1}^s r_i^2 \geq \sum_{i=1}^s a^{-2}r^2d_i^2 = a^{-1}r^2$, as required. It is clear that if $r = 0$, then $\epsilon_r = 0$. For the converse note that we get $\epsilon_r = 0$ if and only if the global minimum tuple is an integer tuple, that is if and only if $a^{-1}rd_i \in \mathbb{Z}$ for all i. But since $d_1 = 1$ (the degree of the trivial irreducible representation), this means that $a^{-1}r \in \mathbb{Z}$. Since $r < a$, this is only possible if $r = 0$.

(ii). By the definition of N from Lemma 3.5, all minimal tuples for n are eligible and there are precisely m_r of them. Moreover, each minimal tuple for n has the form $(kd_1 + r_1',\dots,kd_s+r_s')$, where $(r_1',\dots,r_s')$ is a minimal tuple for r. Now note that for any minimal tuple $(r_1',\dots,r_s')$ for r we have $\sum_{i=1}^s (r_i')^2 = \sum_{i=1}^s r_i^2$, where $(r_1,\dots,r_s)$ is the fixed minimal tuple picked in the statement of the result. Then

$$\begin{aligned}\sum_{i=1}^s (kd_i + r_i')^2 &= k^2\sum_{i=1}^s d_i^2 + 2k\sum_{i=1}^s r_i'd_i + \sum_{i=1}^s (r_i')^2\\ &= k^2a + 2kr + \sum_{i=1}^s r_i^2\\ &= a^{-1}(k^2a^2 + 2akr + r^2) - r^2a^{-1} + \sum_{i=1}^s r_i^2\\ &= a^{-1}n^2 + \epsilon_r.\end{aligned}$$

By Lemma 3.1(iii), the minimal tuples for n give rise to the orbits whose orders are polynomials of maximal degree amongst the orders of all orbits in $X(n,q)$, and the order of each of

these orbits is a polynomial in q with leading term $q^{n^2-a^{-1}n^2-\epsilon_r}$. Since $X(n,q)$ is the disjoint union of all of the orbits it contains, the order of $X(n,q)$ is a polynomial in q with leading term $m_r q^{n^2(1-a^{-1})-\epsilon_r}$. None of the arguments used to derive this result rely on the actual value of q, only that $\mathbb{F}_q$ is a splitting field for A. Since the degrees d_i are all the same for any splitting field, we get the result. □

We summarise the results obtained in the form of an algorithm:

Algorithm. The following steps will allow one to find the numbers m_r, ϵ_r and N from Proposition 3.8, and hence calculate the highest degree term of the polynomial $|X(n,q)|$ for any $n \geq N$.

Step 1. For each $0 \leq r < a$ find all minimal tuples of integers for r; that is, find all tuples $(r_1, \ldots, r_s)$ satisfying $\sum_{i=1}^{s} r_i d_i = r$ and minimising the value of $\sum_{i=1}^{s} r_i^2$. For each r, record the number m_r of minimal tuples found, and the number $\epsilon_r := \sum_{i=1}^{s} r_i^2 - r^2 a^{-1}$, where $(r_1, \ldots, r_s)$ is one of the minimal tuples.

Step 2. Find the smallest $b \in \mathbb{N} \cup \{0\}$ such that $bd_i + r_i \geq 0$ for all r_i from step 1. Then set $N = ba$.

4. Examples

We now present some examples of our algorithm and its results when applied to some groups which are relatively easy to handle. For a given minimal tuple $(r_1, \ldots, r_s)$, we denote $\sum_{i=1}^{s} r_i^2$ by S_r.

4.1. **Abelian groups.** If A is abelian and $\mathbb{F}_q$ is a splitting field for A, then there are a distinct classes of irreducible representations of A and they are all one-dimensional. Therefore, for $0 \leq r < a$, a minimal tuple is just found by filling r spaces with a 1 and $a - r$ with a zero. This means that all minimal tuples are eligible, so $N = 0$, m_r is the binomial coefficient $\binom{a}{r}$, and $S_r = r$. Therefore $\epsilon_r = r - r^2 a^{-1}$ and the leading term of the polynomial $|X(n,q)|$ is $\binom{a}{r} q^{n^2(1-a^{-1})-r+r^2a^{-1}}$.

4.2. **Dihedral groups D_m.** Let $A = D_m$ be the dihedral group of order $a = 2m$. For $\mathbb{F}_q$ to be a splitting field for A, it is enough that $\mathbb{F}_q$ contains all elements of the form $\zeta + \zeta^{-1}$, where ζ is a root of the mth cyclotomic polynomial. Over a splitting field, if m is odd, then A has two irreducible representations of degree 1 and $\frac{m-1}{2}$ of degree 2, and if m is even we get four irreducible representations of degree 1 and $\frac{m-2}{2}$ of degree 2. Hence, we split into two cases:

$m = 2l + 1$ **is odd.** In this case for any even $r = 2k$ with $0 \leq r < 2n$, we choose k of the m representations of degree 2 to come up with a minimal tuple; there are $\binom{m}{k}$ ways to do this, so that is the value of m_r, and $S_r = k = \frac{r}{2}$. For an odd $r = 2k + 1$, we again choose k of the degree 2 representations, and then one of degree 1; there are therefore $m_r = 2\binom{m}{k}$ ways to do this, each one with $S_r = k + 1 = \frac{r+1}{2}$. Hence we have that the leading term of the polynomial $|X(n,q)|$ is $\binom{m}{k} q^{n^2(1-a^{-1})-\frac{r}{2}+r^2a^{-1}}$ if $r = 2k$ is even and $2\binom{m}{k} q^{n^2(1-a^{-1})-\frac{r+1}{2}+r^2a^{-1}}$ if $r = 2k + 1$ is odd.

$m = 2l$ **is even.** In this case for any even $r = 2k$ with $0 \leq r < 2n$, we choose k of the m representations of degree 2 to come up with a minimal tuple; there are $\binom{m}{k}$ ways to do this,

so that is the value of m_r, and $S_r = k = \frac{r}{2}$. For an odd $r = 2k+1$, we again choose k of the degree 2 representations, and then one of degree 1; there are therefore $m_r = 4\binom{m}{k}$ ways to do this, each one with $S_r = k+1 = \frac{r+1}{2}$. Hence we have that the leading term of the polynomial $|X(n,q)|$ is $\binom{m}{k}q^{n^2(1-a^{-1})-\frac{r}{2}+r^2a^{-1}}$ if $r = 2k$ is even and $4\binom{m}{k}q^{n^2(1-a^{-1})-\frac{r+1}{2}+r^2a^{-1}}$ if $r = 2k+1$ is odd.

4.3. **The symmetric group $\mathfrak{S}_4$.** If $A = \mathfrak{S}_4$, which has order $a = 24$, then any field of characteristic not 2 or 3 is a splitting field for A, and the degrees of the irreducible representations over such a field are 1, 1, 2, 3 and 3. According to our algorithm we need to determine the minimal tuples for all $0 \leq r < 24$. The relevant data is summarised in the following table.

r	m_r	sample tuple	S_r	ϵ_r	r	m_r	sample tuple	S_r	ϵ_r
0	1	$(0,0,0,0,0)$	0	0	12	4	$(1,0,1,2,1)$	7	1
1	2	$(1,0,0,0,0)$	1	$\frac{23}{24}$	13	2	$(1,1,1,2,1)$	8	$\frac{23}{24}$
2	1	$(0,1,0,0,0)$	1	$\frac{5}{6}$	14	1	$(0,0,1,2,2)$	9	$\frac{5}{6}$
3	2	$(0,0,0,1,0)$	1	$\frac{5}{8}$	15	2	$(1,0,1,2,2)$	10	$\frac{5}{8}$
4	4	$(1,0,0,1,0)$	2	$\frac{4}{3}$	16	1	$(1,1,1,2,2)$	11	$\frac{1}{3}$
5	2	$(0,0,1,1,0)$	2	$\frac{23}{24}$	17	2	$(1,0,2,2,2)$	13	$\frac{23}{24}$
6	1	$(0,0,0,1,1)$	2	$\frac{1}{2}$	18	1	$(1,1,2,2,2)$	14	$\frac{1}{2}$
7	2	$(1,0,0,1,1)$	3	$\frac{23}{24}$	19	2	$(1,1,1,3,2)$	16	$\frac{23}{24}$
8	1	$(0,0,1,1,1)$	3	$\frac{1}{3}$	20	4	$(1,0,2,3,2)$	18	$\frac{4}{3}$
9	2	$(1,0,1,1,1)$	4	$\frac{5}{8}$	21	2	$(1,1,2,3,2)$	19	$\frac{5}{8}$
10	1	$(1,1,1,1,1)$	5	$\frac{5}{6}$	22	1	$(1,1,1,3,3)$	21	$\frac{5}{6}$
11	2	$(0,0,1,2,1)$	6	$\frac{23}{24}$	23	2	$(1,0,2,3,3)$	23	$\frac{23}{24}$

Of note here is the fact that in this case for every r all the minimal tuples are eligible tuples, and hence for this example the value of $N = 0$ (so our result is valid for all n). It is relatively straightforward to show that this is a general phenomenon which occurs when the degrees of the irreducible representations for A can be put into an ordered list $1 = d_1 \leq d_2 \leq \cdots \leq d_s$ with $d_i - d_{i-1} \leq 1$ for $1 < i \leq s$.

It is also worth noting that this small example already shows that the value of the "error term" ϵ_r can be greater than 1, so finding the degree of the polynomial $|X(n,q)|$ is more complicated than simply taking the integer part of $n^2(1-a^{-1})$.

4.4. **Further Examples.** Let $A = \mathfrak{S}_5$, so $a = 120$. Any field of characteristic larger than 5 is a splitting field for $\mathfrak{S}_5$, and the degrees of the irreducible representations over such a field are $1, 1, 4, 4, 5, 5$ and 6. When $r = 3$, the tuple $(0, -1, 1, 0, 0, 0, 0)$ is one of four minimal tuples (the others being those naturally obtained from this one by permuting amongst entries of equal degree). Hence we cannot take $N = 0$ as we have negative entries for at least one value of r. In this case, the value of N provided by our algorithm is $N = a = 120$. For similar

reasons, when $A = \mathfrak{S}_6$, we also need to go up to $N = a = 720$. We have also calculated directly that value of N for all groups of order $a \leq 80$ is either 0 or a.

5. Extensions and Further Remarks

In this section we outline various ways to extend the work presented, either by relaxing some of the standing assumptions made in Section 2 or by changing the groups involved. We also point out an application of this work to the study of representation varieties. We begin by discussing the restrictions we have placed on the field $\mathbb{F}_q$.

5.1. **The assumption that $\mathbb{F}_q$ is a splitting field.** We have had the standing assumption that $\mathbb{F}_q$ is a splitting field for A. This means, in particular, that the characteristic p of $\mathbb{F}_q$ is coprime to the size a of the group A and that every irreducible $\mathbb{F}_qA$-module is absolutely irreducible. This assumption allows us to assume that all modules encountered are semisimple and that the irreducible summands encountered do not really depend on the field in any essential way.

Suppose we relax the assumption that all irreducible modules are absolutely irreducible, but retain for now the assumption that q and a are coprime (this is the situation in [5], for example). Then we can still write down a basic set $(N_1, \ldots, N_t)$, say, of irreducible $\mathbb{F}_qA$-modules. It follows from Schur's Lemma that $\mathrm{End}_{\mathbb{F}_qA-\mathrm{mod}}(N_i)$ is a division ring for each i, and since any finite division ring is a field it is not hard to see that we have $\mathrm{End}_{\mathbb{F}_qA-\mathrm{mod}}(N_i) \simeq \mathbb{F}_{q^{e_i}}$ for some $e_i \geq 1$. Moreover, if we extend scalars to $\mathbb{F}_{q^{e_i}}$, then the module N_i splits into a direct sum of e_i absolutely irreducible $\mathbb{F}_{q^{e_i}}A$-modules, $(M_{i1}, \ldots, M_{ie_i})$ say, which form a single orbit under the action of the Galois group $\mathrm{Gal}(\mathbb{F}_{q^{e_i}}/\mathbb{F}_q) \simeq \mathbb{Z}_{e_i}$. Denote the dimension of each M_{ij} over $\mathbb{F}_{q^{e_i}}$ by d_{ij}, and note that $d_{ij} = d_{i1}$ for all $1 \leq j \leq e_i$. Note also that the $\mathbb{F}_q$-dimension of N_i must be $d_{i1}e_i$. Conversely, given an absolutely irreducible $\mathbb{F}_{q^e}A$-module M over some extension $\mathbb{F}_{q^e}$ of $\mathbb{F}_q$, taking the direct sum of the distinct $\mathrm{Gal}(\mathbb{F}_{q^e}/\mathbb{F}_q)$- conjugates of M forms a module which arises from precisely one of the N_i by extension of scalars from $\mathbb{F}_q$ to $\mathbb{F}_{q^e}$. For justification of the claims above, see results in [3, Sec. 7], in particular Cor. 7.11 and Prop. 7.18.

In this way, one can retrieve all of the information necessary to mimic the proofs and constructions in Section 3 over $\mathbb{F}_q$. In particular, the degrees d_{ij} occurring above (with their multiplicities e_i) are precisely the degrees of the distinct representatives of the isomorphism classes of absolutely irreducible KA-modules over some sufficiently large extension K of $\mathbb{F}_q$ (it suffices to extend to a finite field containing all the $\mathbb{F}_{q^{e_i}}$). We therefore have that $\sum_{i=1}^{t}\sum_{j=1}^{e_i} d_{ij}^2 = a$. Within this set-up, one can still calculate stabilisers of representations – we see direct products of $\mathrm{GL}_n(q^{e_i})$s – and one can analyse t-tuples of integers $(m_1, \ldots, m_t)$ such that $\sum_{i=1}^{t} m_i d_{i1} e_i = n$. This amounts to the same thing as analysing those s-tuples of integers $(n_{11}, \ldots, n_{te_t})$ such that $\sum_{i=1}^{s}\sum_{j=1}^{e_i} n_{ij}d_{ij} = n$ subject to the additional constraint that $n_{i1} = n_{ij}$ for all $1 \leq j \leq e_i$. Presenting it in this way shows that, given the degrees d_{ij}, we actually need to identify a subset of the eligible s-tuples for the number n from Section 3 – those tuples satisfying the given additional constraint. The analysis in Section 3 now proceeds almost unchanged: certain of these tuples will be minimal, and after a certain point, all minimal tuples will be eligible. After this point, the leading coefficient and power of q in the polynomial $|X(n, q)|$ will only depend on the value of n modulo a. Furthermore, when n is divisible by a, the unique minimal tuple described in the proof of Proposition

3.8(i) actually satisfies the additional constraint given, so we get a leading term $q^{n^2(1-a^{-1})}$ in this case.

The preceding remarks are perhaps made more transparent with a couple of simple examples. We maintain notation from previous sections.

Example 5.1. Let d be an odd positive integer, let $q = 2^d$, and let A be the cyclic group of order 3, generated by the element x of order 3, say. We need three distinct cube roots of 1 to realise all the absolutely irreducible representations of A; since d is odd, $\mathbb{F}_q$ does not contain three distinct cube roots of 1, but $\mathbb{F}_{q^2}$ does. Over $\mathbb{F}_q$, A has the trivial representation N_1 and another irreducible representation N_2 of degree 2; N_2 can be realised concretely by sending x to the matrix $\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$ (note that this matrix does have order 3 when the characteristic is 2, and it has characteristic polynomial $X^2 + X + 1$, so is not diagonalisable unless the field contains a nontrivial cube root of 1). If we extend scalars by adjoining a root of $X^2 + X + 1$ (i.e., move to the field $\mathbb{F}_{q^2}$), then N_2 splits into two one-dimensional modules.

Now, we have only have one representation of A over $\mathbb{F}_q$ of degree 1 – the trivial representation – so we have in this case that that $|X(1, q)| = 1$. On the other hand, if we extend scalars to $\mathbb{F}_{q^2}$, we get $|X(1, q^2)| = 3$. In fact, for any $n \in \mathbb{N}$, we have

$$|X(3n + 1, q)| = q^{\frac{2}{3}(3n+1)^2 - \frac{2}{3}} + \text{ lower order terms},$$

whereas

$$|X(3n + 1, q^2)| = 3(q^2)^{\frac{2}{3}(3n+1)^2 - \frac{2}{3}} + \text{ lower order terms}.$$

This shows how the leading coefficient of $|X(n, q)|$ can vary with q when we work with fields which are not necessarily splitting fields.

Example 5.2. Let $q = 3$ and let A be the dihedral group of order 10. Over $\mathbb{F}_3$ there are three irreducible representations of A: two of dimension 1, N_1 and N_2, say, and a single 4-dimensional representation, say N_3. If we extend scalars to $\mathbb{F}_9$, then N_4 splits into the two familiar two-dimensional representations (those we see "generically" by considering dihedral groups as groups of plane rotations and reflections); call these two-dimensional modules M_3 and M_3', and denote the modules given by N_1 and N_2 after extension of scalars by M_1 and M_2.

Over $\mathbb{F}_3$ there are four ways to build a representation of degree 3 – $N_1 \oplus N_1 \oplus N_1$ or $N_1 \oplus N_1 \oplus N_2$ or $N_1 \oplus N_2 \oplus N_2$ or $N_2 \oplus N_2 \oplus N_2$ – and amongst these the middle two correspond to minimal tuples. For these, the value of our error term $\epsilon_r = 1^2 + 2^2 - \frac{9}{10} = \frac{21}{10}$. On the other hand, if we work over $\mathbb{F}_9$, then we can build a 3-dimensional representation $M_1 \oplus M_3$, for example, for which the error term is $1^2 + 1^2 - \frac{9}{10} = \frac{11}{10}$. Hence, whenever n is congruent to 3 modulo 10,

$$\deg(|X(n, 3)|) = \frac{9}{10}n^2 - \frac{21}{10},$$

whereas

$$\deg(|X(n, 9)|) = \frac{9}{10}n^2 - \frac{11}{10}.$$

This shows how the degree of the polynomial $|X(n, q)|$ can vary with q when we work with fields which are not necessarily splitting fields.

Progress is even possible if we drop the assumption that q and a are coprime, so that not all $\mathbb{F}_q A$-modules are semisimple. Some sort of semisimplicity assumption is necessary, as is shown by [5, Example 1], but it is possible to make progress in the modular case if one is willing to replace the set $\mathrm{Hom}(A, \mathrm{GL}_n(q))$ with the set $\mathrm{Hom}_{cr}(A, \mathrm{GL}_n(q))$ of all homomorphisms from A to $\mathrm{GL}_n(q)$ such that the associated representation is semisimple (completely reducible); this is the standing assumption in the paper [1], for example. If one does this, then similar results are possible to those in Section 3, but one has to work a bit harder. For example, instead of results depending on a, one has to use the dimension of the socle of the group algebra $\mathbb{F}_q A$ (denote this dimension by b), and one cannot hope for the results obtained to be independent of q. However, one should still expect that the leading term of the polynomial $|\mathrm{Hom}_{cr}(A, \mathrm{GL}_n(q))|$ will have the form $m_r q^{n^2(1-b^{-1})-\epsilon_r}$, where r is the value of n modulo b, and m_r and ϵ_r can be determined by procedures similar to those laid out in Secion 3.

5.2. **Changing the target group.** The main point of the paper [1] is to produce bounds similar to those in [5], replacing $\mathrm{GL}_n(q)$ with a unitary, symplectic or orthogonal group, see [1, Thm. B, Thm. C, Thm. D]. This is achieved at the expense of knowing a bit more information about the simple modules for the group A; for example, one needs to know how many of the simple modules are self-dual. However, armed with this knowledge, an approach similar to that given in this note would produce similar results for these cases too.

5.3. **Dimensions of representation varieties.** Let K be an algebraically closed field, and let $G = \mathrm{GL}_n(K)$. The set $X := \mathrm{Hom}(A, G)$ of homomorpisms from A to G is an example of a *representation variety* [4] (it can be realised as a closed subvariety of the a-fold cartesian product G^a). The linear algebraic group G acts on X by restriction of the simultaneous conjugation action on G^a and, as is observed in [5, Sec. 2], under the assumption that K has characteristic zero or coprime to a, the G-orbits in X are the irreducible components of X. The dimension of such an orbit is the dimension of G minus the dimension of the associated stabilizer. The analysis in this paper shows that the maximal dimension arising is precisely $n^2(1 - a^{-1}) - \epsilon_r$, where the notation is that in Proposition 3.8, and this is therefore the dimension of X. Moreover, the number m_r is precisely the number of irreducible components of maximal dimension in X.

References

[1] M.E. Bate, *The number of homomorphisms from finite groups to classical groups*, J. Algebra **308** (2007), no. 2, 612-628.

[2] N. Chigira, Y. Takegahara, T. Yoshida, *On the number of homomorphisms from a finite group to a general linear group*, J. Algebra **232** (2000), no. 1, 236–254.

[3] C.W. Curtis, I. Reiner, *Methods of representation theory – with applications to finite groups and orders*, Vol. I, Wiley, New York, 1981.

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

[5] M.W. Liebeck, A. Shalev, *The Number of Homomorphisms from A Finite Group To a General Linear Group*, Communications in Algebra **32** (2004), 657–661.

Department of Mathematics, University of York, York YO10 5DD. United Kingdom
E-mail address: michael.bate@york.ac.uk

Department of Mathematics, Lancaster University, Lancaster, LA1 4YF, United Kingdom
E-mail address: a.gullon@lancaster.ac.uk