www.theoryofgroups.ir

International Journal of Group Theory
ISSN (print): 2251-7650, ISSN (on-line): 2251-7669
Vol. 8 No. 4 (2019), pp. 11-28.

www.ui.ac.ir

GRAHAM HIGMAN'S PORC THEOREM

MICHAEL VAUGHAN-LEE

Communicated by Gunnar Traustason

Abstract. Graham Higman published two important papers in 1960. In the first of these papers he proved that for any positive integer n the number of groups of order p^n is bounded by a polynomial in p, and he formulated his famous PORC conjecture about the form of the function $f(p^n)$ giving the number of groups of order p^n. In the second of these two papers he proved that the function giving the number of p-class two groups of order p^n is PORC. He established this result as a corollary to a very general result about vector spaces acted on by the general linear group. This theorem takes over a page to state, and is so general that it is hard to see what is going on. Higman's proof of this general theorem contains several new ideas and is quite hard to follow. However in the last few years several authors have developed and implemented algorithms for computing Higman's PORC formulae in special cases of his general theorem. These algorithms give perspective on what are the key points in Higman's proof, and also simplify parts of the proof.

In this note I give a proof of Higman's general theorem written in the light of these recent developments.

1. Introduction

Graham Higman wrote two immensely important and influential papers on enumerating p-groups in the late 1950s. The papers were entitled *Enumerating p-groups* I and II, and were published in the Proceedings of the London Mathematical Society in 1960 (see [4] and [5]). In the first of these papers

MSC(2010): Primary: 20D15; Secondary: 17B30.

Keywords: PORC; p-group; enumerate.

Received: 17 August 2018, Accepted: 19 September 2018.

http://dx.doi.org/10.22108/ijgt.2018.112574.1498

.

Higman proves that if we let $f(p^n)$ be the number of p-groups of order p^n, then

$$p^{\frac{2}{27}n^2(n-6)} \leq f(p^n) \leq p^{(\frac{2}{15}+\varepsilon_n)n^3},$$

where ε_n tends to zero as n tends to infinity. Higman also formulated his famous PORC conjecture concerning the form of the function $f(p^n)$. He conjectured that for each n there is an integer N (depending on n) such that for p in a fixed residue class modulo N the function $f(p^n)$ is a polynomial in p. For example, for $p \geq 5$ the number of groups of order p^6 is

$$3p^2 + 39p + 344 + 24\gcd(p-1,3) + 11\gcd(p-1,4) + 2\gcd(p-1,5).$$

(See [7].) So for $p \geq 5$, $f(p^6)$ is one of 8 polynomials in p, with the choice of polynomial depending on the residue class of p modulo 60. The number of groups of order p^6 is **P**olynomial **O**n **R**esidue **C**lasses. In [5] Higman proved that, for any given n, the function enumerating the number of p-class 2 groups of order p^n is a PORC function of p. He obtained this result as a corollary to a very general theorem about vector spaces acted on by the general linear group. As another corollary to this general theorem, he also proved that for any given n the function enumerating the number of algebras of dimension n over the field of q elements is a PORC function of q.

In recent years several authors have developed algorithms for computing Higman's PORC formulae in various applications of his general theorem. Witty [11] wrote a thesis describing an algorithm for computing the number of r-generator p-class two groups, and I have published a series of papers on this topic and on computing the numbers of non-associative algebras of dimension d ([8], [9], [10]). Eick and Wesche [2] describe an algorithm for computing the numbers of associative algebras over a finite field which are nilpotent of class 2, and this algorithm has been implemented in GAP. These algorithms simplify parts of Higman's theory, and have given me a better understanding of his general theorem and its proof. In this note I offer my insights into Higman's remarkable theorem.

2. Algebraic families of groups

Higman introduces the notion of an *algebraic family of groups*. Let $\mathbb{Q}$ be the rational field and suppose we have a homomorphism

$$\varphi : \mathrm{GL}(m,\mathbb{Q}) \to \mathrm{GL}(n,\mathbb{Q})$$

with the property that if A is a matrix in $\mathrm{GL}(m,\mathbb{Q})$ then $\varphi(A)$ is a matrix in $\mathrm{GL}(n,\mathbb{Q})$ with entries of the form $\frac{r}{s}$ where r and s are polynomials over $\mathbb{Q}$ in the entries of A. (Of course the polynomials r, s should depend only on φ and not on A.) Paraphrasing Higman slightly, he writes "Of course, the least common multiple of the denominators s is a power of $\det(A)$". This stumped me for quite a while, but eventually I consulted an expert in algebraic groups who assured me that this was a well known, basic fact. In the end I managed to find my own elementary proof of this, but I have decided not to include my proof in this note. So we assume that the entries in $\varphi(A)$ are of the form $\frac{r}{\det(A)^k}$ where r is a polynomial over $\mathbb{Q}$ in the entries of A.

http://dx.doi.org/10.22108/ijgt.2018.112574.1498

Higman's idea is that if K is any field whose characteristic does not divide the denominator of any of the coefficients in the polynomials giving the entries in $\varphi(A)$ then the coefficients in these polynomials can be interpreted as elements of the prime subfield of K so that φ defines a homomorphism

$$\varphi_K : \mathrm{GL}(m, K) \to \mathrm{GL}(n, K).$$

Higman calls the collection of images $\varphi_K(\mathrm{GL}(m, K))$ an algebraic family of groups.

Now let $\varphi : \mathrm{GL}(m, \mathbb{Q}) \to \mathrm{GL}(n, \mathbb{Q})$ give an algebraic family of groups, and let P be the (finite) set of primes which divide denominators of coefficients in the polynomials giving the entries in $\varphi(A)$. Suppose that K is a finite field of order q, where the characteristic of K is not contained in P. Let V be a vector space of dimension n over K. Then φ_K gives us an action of $\mathrm{GL}(m, K)$ on V. Higman [5] proves the following theorem.

Theorem 2.1. *(a) The number of orbits of V under the action of $GL(m, K)$, considered as a function of q, is PORC.*

(b) For each integer k with $0 \leq k \leq n$, the number of orbits of $GL(m, K)$ on subspaces of V of dimension k, considered as a function of q, is PORC.

Actually Higman's algebraic families of groups are more general than this, as they are given by homomorphisms

$$\varphi : \mathrm{GL}(m_1, \mathbb{Q}) \times \mathrm{GL}(m_2, \mathbb{Q}) \times \cdots \times \mathrm{GL}(m_r, \mathbb{Q}) \to \mathrm{GL}(n, \mathbb{Q}).$$

It may be that Higman's main reason for this generalization is that he proves (b) (for $r = 1$) by considering the action of $\mathrm{GL}(k, K) \times \mathrm{GL}(m, K)$ on the space of $k \times n$ matrices, with $\mathrm{GL}(k, K)$ acting on the left by matrix multiplication, and $\mathrm{GL}(m, K)$ acting on the right via φ_K. So to prove (b) for $r = 1$ he proves (a) for $r = 2$, and more generally to prove (b) for a direct product of r general linear groups he proves (a) for a direct product of $r+1$ general linear groups. The proof of Higman's theorem given below avoids this complication, so I will restrict my attention to the case $r = 1$. Nevertheless the proof given here can easily be adapted to prove Theorem 2.1 for Higman's more general algebraic families, the only difference being that the notation would be more complicated.

3. Two examples of algebraic families of groups

3.1. **GL(V) acting on $V \wedge V$.** Suppose that V is a vector space of dimension n over a field K. Then there is a natural action of $\mathrm{GL}(V)$ on the exterior square $V \wedge V$, which we can describe as follows.

Suppose that V has basis $v_1, v_2, \ldots, v_n$ over K, and let $g \in \mathrm{GL}(V)$ have matrix $A = [a_{ij}]$ with respect to this basis, so that $v_i g = \sum_j a_{ij} v_j$. Then $V \wedge V$ has a basis consisting of the elements $v_i \wedge v_j$ with $i < j$, and

$$(v_i \wedge v_j)g = \sum_{k,m} a_{ik}a_{jm}(v_k \wedge v_m) = \sum_{k<m} (a_{ik}a_{jm} - a_{im}a_{jk})(v_k \wedge v_m).$$

So the matrix giving the action of g on $V \wedge V$ with respect to the basis $v_i \wedge v_j$ with $i < j$ has entries of the form $a_{ik}a_{jm} - a_{im}a_{jk}$. We have a homomorphism

$$\varphi : GL(n, K) \to GL(\binom{n}{2}, K)$$

and if $A \in \mathrm{GL}(n, K)$ then the entries in $\varphi(A)$ are integer polynomials in the entries of A. So we have an algebraic family of groups. Theorem 2.1 implies that if K is a field of order q then the number of orbits of $\mathrm{GL}(n, K)$ on $V \wedge V$ is PORC as a function of q, as is the number of orbits of $\mathrm{GL}(n, K)$ on subspaces of $V \wedge V$ of dimension k ($0 \leq k \leq \binom{n}{2}$).

3.2. **Algebras over a field K.** Higman's general theorem also implies that for every dimension m the number of algebras of dimension m over a field K of order q is a PORC function of q. (See [9].) By "algebra" we mean a vector space with a bilinear product. There is no requirement that the product satisfy any other condition such as associativity. If B is an algebra of dimension m over K, and if we pick a basis $v_1, v_2, \ldots, v_m$ for B as a vector space over K then for each pair of basis elements v_i, v_j we can express the product v_iv_j as a linear combination

$$v_iv_j = \sum_k \lambda_{ijk}v_k$$

for some scalars $\lambda_{ijk} \in K$. These scalars are *structure constants* for the algebra B, and completely determine B. If we pick another basis $w_1, w_2, \ldots, w_m$, and if

$$w_iw_j = \sum_k \mu_{ijk}w_k$$

then we obtain another set of structure constants μ_{ijk}. We can express the elements of the second basis as linear combinations of elements of the first basis, and vice versa:

$$w_i = \sum_{j=1}^{m} a_{ji}v_j \ (1 \leq i \leq m),$$
$$v_j = \sum_{k=1}^{m} b_{kj}w_k \ (1 \leq j \leq m),$$

where $[a_{ji}]$ and $[b_{kj}]$ are $m \times m$ matrices over K which are inverse to each other. So

$$\begin{aligned} w_iw_j &= \sum_{r,s=1}^{m} a_{ri}a_{sj}v_rv_s \\ &= \sum_{r,s,t=1}^{m} a_{ri}a_{sj}\lambda_{rst}v_t \\ &= \sum_{r,s,t,k=1}^{m} a_{ri}a_{sj}\lambda_{rst}b_{kt}w_k. \end{aligned}$$

http://dx.doi.org/10.22108/ijgt.2018.112574.1498

It follows that

$$\mu_{ijk} = \sum_{r,s,t=1}^{n} a_{ri}a_{sj}\lambda_{rst}b_{kt}.$$

If we think of the sets of structure constants as vectors in an m^3 dimensional vector space over K then this gives us a homomorphism from $\mathrm{GL}(m,K)$ into $\mathrm{GL}(m^3,K)$ where the image of a matrix A in $\mathrm{GL}(m,K)$ has entries of the form $\frac{f}{\det A}$ where f is an integer polynomial in the entries of A. Two sets of structure constants give isomorphic algebras if and only if they lie in the same orbit under the action of $\mathrm{GL}\,(m,K)$, and so Theorem 2.1 (a) implies that the number of m-dimensional algebras over K, considered as a function of $q = |K|$, is PORC.

4. Diagonal matrices in GL$(m,\mathbb{Q})$

Let $\varphi : \mathrm{GL}(m,\mathbb{Q}) \to \mathrm{GL}(n,\mathbb{Q})$ give an algebraic family of groups. If $A \in \mathrm{GL}(m,\mathbb{Q})$ then the entries in $\varphi(A)$ have the form $\frac{r}{\det(A)^k}$ where r is a polynomial over $\mathbb{Q}$ in the entries of A, and we let P be the finite set of primes which divide denominators of coefficients in the polynomials r. Let R be the ring of rationals of the form $\frac{a}{b}$ where only primes in P divide b.

Theorem 4.1. *There is a matrix Q with entries in R and with $\det Q = \pm 1$ such that if A is a diagonal matrix in $GL(m,\mathbb{Q})$ then $Q^{-1}\varphi(A)Q$ is diagonal. Furthermore, if A has eigenvalues $\lambda_1, \lambda_2, \ldots, \lambda_m$ then $\varphi(A)$ has eigenvalues of the form $\lambda_1^{n_1}\lambda_2^{n_2}\cdots\lambda_m^{n_m}$ for some integers n_i.*

To my mind this is the cleverest and trickiest part of Higman's proof of Theorem 2.1. But note that in the case of the two examples given in Section 3 there is nothing to prove. In the first example $\varphi(A)$ is diagonal with eigenvalues $\lambda_i\lambda_j$ $(i < j)$, and in the second example $\varphi(A)$ is diagonal with eigenvalues $\frac{\lambda_i\lambda_j}{\lambda_k}$ $(i,j,k = 1,2,\ldots,m)$. Similarly in Eick and Wesche's algorithm [2] to compute the numbers of class two associative algebras they consider the action of $\mathrm{GL}(V)$ on $V \otimes V$, and in this case if A is diagonal with eigenvalues $\lambda_1, \lambda_2, \ldots, \lambda_m$ then $\varphi(A)$ is diagonal with eigenvalues $\lambda_i\lambda_j$ $(i,j = 1,2,\ldots,m)$. Of course this is only true if we choose the "right" basis for $V \otimes V$. Theorem 4.1 implies that if we have an algebraic family of groups giving an action of $\mathrm{GL}(m,\mathbb{Q})$ on a vector space W, then we can always choose a basis of W with respect to which diagonal matrices in $\mathrm{GL}(m,\mathbb{Q})$ act diagonally on W.

Let $A \in \mathrm{GL}(m,\mathbb{Q})$ be a diagonal matrix with eigenvalues $\lambda_1, \lambda_2, \ldots, \lambda_m$. The entries in $\varphi(A)$ are R-linear combinations of products $\lambda_1^{n_1}\lambda_2^{n_2}\cdots\lambda_m^{n_m}$ with $n_i \in \mathbb{Z}$. Let $\lambda_1^{n_{i1}}\lambda_2^{n_{i2}}\cdots\lambda_m^{n_{im}}$ $(1 \le i \le k)$ be the distinct products of eigenvalues of A and their inverses which occur in $\varphi(A)$. We can write

$$\varphi(A) = \sum_{i=1}^{k} E_i\lambda_1^{n_{i1}}\lambda_2^{n_{i2}}\cdots\lambda_m^{n_{im}},$$

http://dx.doi.org/10.22108/ijgt.2018.112574.1498

where $E_1, E_2, \ldots, E_k$ are $n \times n$ matrices with entries in R. If we let B be a diagonal matrix in $\mathrm{GL}(m, \mathbb{Q})$ with eigenvalues $\mu_1, \mu_2, \ldots, \mu_m$ then

$$\varphi(B) = \sum_{i=1}^{k} E_i \mu_1^{n_{i1}} \mu_2^{n_{i2}} \cdots \mu_m^{n_{im}}$$

and

$$\varphi(AB) = \sum_{i=1}^{k} E_i (\lambda_1 \mu_1)^{n_{i1}} (\lambda_2 \mu_2)^{n_{i2}} \cdots (\lambda_m \mu_m)^{n_{im}}.$$

Since $\varphi(A)\varphi(B) = \varphi(AB)$ for all $\lambda_1, \lambda_2, \ldots, \lambda_m, \mu_1, \mu_2, \ldots, \mu_m \in \mathbb{Q} \setminus \{0\}$ this implies that $E_i E_j = 0$ for all $i \neq j$ and that $E_i^2 = E_i$ for all i.

So the matrices $E_1, E_2, \ldots, E_k$ can be simultaneously diagonalized. This means that we can find a non-singular $n \times n$ matrix C such that every column of C is an eigenvector with eigenvalue 0 or 1 for each of $E_1, E_2, \ldots, E_k$. We can take the entries in C to be integers. Since $E_i E_j = 0$ for $i \neq j$ and since $\varphi(A)$ is non-singular, each column of C has eigenvalue 1 for exactly one of the matrices $E_1, E_2, \ldots, E_k$. We can order the columns of C so that the first few columns are eigenvectors with eigenvalue 1 for E_1, so that the next few columns are eigenvectors with eigenvalue 1 for E_2, and so on. For $i = 1, 2, \ldots, n$ let e_i be the column vector with 1 in the i^{th} place, and 0 in every other place.

We consider elementary row operations on C of the following three forms:

(1) Swap two rows.
(2) Subtract an integer multiple of one row from another.
(3) Multiply a row by -1.

If a is the greatest common divisor of the entries in the first column of C then we can apply a sequence of row operations to reduce the first column of C to ae_1. Then we can apply a sequence of row operations to rows $2, 3, \ldots, n$ to reduce the second column of C to $be_1 + ce_2$ for some b, c. Next we apply a sequence of row operations to rows $3, 4, \ldots, n$ to reduce the third column to $de_1 + ee_2 + fe_3$ for some d, e, f. Continuing in this way we eventually reduce C to an upper triangular integer matrix. Applying this sequence of row operations to C corresponds to premultiplying C by a sequence of elementary matrices. Multiplying these elementary matrices together we obtain an integer matrix Q with $\det Q = \pm 1$ such that QC is upper triangular. Let $QC = D$ and let $F_i = QE_iQ^{-1}$ for $i = 1, 2, \ldots, k$. Then $F_i F_j = 0$ for $i \neq j$ and $F_i^2 = F_i$ for all i. Let $V_i = \ker(F_i - 1)$ and let $\dim V_i = d_i$ for $i = 1, 2, \ldots, k$. Then the first d_1 columns of D form a basis for V_1, the next d_2 columns of D form a basis for V_2, and so on. However

- the first d_1 columns of D span the same space as $e_1, e_2, \ldots, e_{d_1}$,
- the next d_2 columns span the same space as

$$e_{d_1+1} + v_1, e_{d_1+2} + v_2, \ldots, e_{d_1+d_2} + v_{d_2}$$

for some $v_1, v_2, \ldots, v_{d_2} \in V_1$,

- the next d_3 columns span the same space as

  $$e_{d_1+d_2+1}+w_1, e_{d_1+d_2+2}+w_2, \dots, e_{d_1+d_2+d_3}+w_{d_3}$$

  for some $w_1, w_2, \dots, w_{d_3} \in V_1+V_2$,
- and so on.

Now let E be the $n \times n$ matrix with columns

$$e_1, e_2, \dots, e_{d_1}, e_{d_1+1}+v_1, \dots, e_{d_1+d_2}+v_{d_2}, e_{d_1+d_2+1}+w_1, \dots, e_{d_1+d_2+d_3}+w_{d_3}, \dots,$$

so that the first d_1 columns of E form a basis for V_1, the next d_2 columns form a basis for V_2, and so on. Then

$$e_{d_1+1}+v_1 = F_2(e_{d_1+1}+v_1) = F_2 e_{d_1+1}$$

since $F_1F_2 = 0$. All the entries in the matrix F_2 lie in R, and so all the entries in v_1 lie in R. Similarly, all the entries in $v_2, v_3, \dots, v_{d_2}, w_1, \dots, w_{d_3}, \dots$ lie in R. So E is an upper triangular matrix with 1's down the diagonal and with all the entries above the diagonal lying in the ring R. It follows that $Q^{-1}E$ is a matrix with entries in R and with determinant ± 1, and such that $E^{-1}Q\varphi(A)Q^{-1}E$ is diagonal. This completes the proof of Theorem 4.1.

From now on we replace $\varphi : \mathrm{GL}(m,\mathbb{Q}) \to \mathrm{GL}(n,\mathbb{Q})$ by φ^*, where

$$\varphi^*(A) = E^{-1}Q\varphi(A)Q^{-1}E.$$

In other words, we assume that $\varphi(A)$ is diagonal whenever A is diagonal.

5. Matrices in Jordan form

For each integer $k \geq 1$ let J_k be the $k \times k$ Jordan matrix with 1's down the diagonal and 1's down the superdiagonal. Higman considers a non-singular matrix to be in Jordan form if it can be expressed in the form

$$\lambda_1 J_{k_1} \oplus \lambda_2 J_{k_2} \oplus \cdots \oplus \lambda_r J_{k_r} \tag{5.1}$$

for some eigenvalues $\lambda_1, \lambda_2, \dots, \lambda_r$ and some integers $k_1, k_2, \dots, k_r$. (This is possible since the eigenvalues are non-zero.) So let $A \in \mathrm{GL}(m,\mathbb{Q})$ be a matrix of form (5.1). For the moment assume that the eigenvalues $\lambda_1, \lambda_2, \dots, \lambda_r$ are all distinct. Actually, it helps to think of $\lambda_1, \lambda_2, \dots, \lambda_r$ as indeterminates. Let

$$\Lambda = \lambda_1 I_{k_1} \oplus \lambda_2 I_{k_2} \oplus \cdots \oplus \lambda_r I_{k_r},$$
$$J = J_{k_1} \oplus J_{k_2} \oplus \cdots \oplus J_{k_r}.$$

Then $A = \Lambda J = J\Lambda$. By Theorem 4.1 we may suppose that $\varphi(\Lambda)$ is diagonal, with eigenvalues which are products of the eigenvalues $\lambda_1, \lambda_2, \dots, \lambda_r$ and their inverses. Suppose that the products that arise as eigenvalues of $\varphi(\Lambda)$ are $m_1, m_2, \ldots, m_s$, and let Q be a permutation matrix chosen so that

$$L = Q^{-1}\varphi(\Lambda)Q = m_1 I_{t_1} \oplus m_2 I_{t_2} \oplus \cdots \oplus m_s I_{t_s}$$

for some positive integers $t_1, t_2, \ldots, t_s$. Let $M = Q^{-1}\varphi(J)Q$. Then $LM = ML$ and so

$$M = E_1 \oplus E_2 \oplus \cdots \oplus E_s$$

where E_i is a $t_i \times t_i$ matrix for $i = 1, 2, \ldots, s$, and where the entries in E_i all lie in R . The matrix J is conjugate to all its power J^i $(i = 1, 2, \ldots)$ and so M is also conjugate to all its powers. This implies that 1 is the only eigenvalue of M. And this implies that we can find invertible matrices $X_1, X_2, \ldots, X_s$ with rational entries such that $X_i^{-1}E_iX_i$ is in Jordan form (with 1 as the only eigenvalue) for $i = 1, 2, \ldots, s$. Let

$$X = X_1 \oplus X_2 \oplus \cdots \oplus X_s.$$

So

$$X^{-1}Q^{-1}\varphi(A)QX = LX^{-1}MX \tag{5.2}$$

is in Jordan form. Note that the matrices Q, X do not depend on the values of $\lambda_1, \lambda_2, \ldots, \lambda_r$. Furthermore $LX^{-1}MX$ is in Jordan form even if $\lambda_1, \lambda_2, \ldots, \lambda_r$ are not all distinct. Now suppose that p is a prime which does not divide the denominator of any of the entries in X and does not divide the numerator of $\det X$. If K is a finite field of characteristic p then we can interpret X and Q as non singular matrices with entries in the prime subfield of K, so equation (5.2) also gives the Jordan form of $\varphi_K(A)$ if A is a matrix in $\mathrm{GL}(m, K)$ of the form (5.1). Note that the sizes of the Jordan blocks in $X^{-1}MX$ and the number of blocks of each size depends only on the integers $k_1, k_2, \ldots, k_r$. Also the eigenvalues of $\varphi_K(A)$ corresponding to the Jordan blocks in $X^{-1}MX$ have the form

$$m_i = \lambda_1^{n_{i1}}\lambda_2^{n_{i2}} \cdots \lambda_r^{n_{ir}}$$

for some integers n_{ij} which depend only on $k_1, k_2, \ldots, k_r$.

There will be a finite number of "exceptional" characteristics which divide one of the denominators of the entries in X, or divide the numerator of $\det X$. Let K be a finite field with exceptional characteristic p. Let A be a matrix in $\mathrm{GL}(m, K)$ of the form (5.1). We follow the same analysis as above and obtain the same expression

$$Q^{-1}\varphi_K(A)Q = LM = ML$$

as above. Now $J^{p^m} = I_m$, and this implies that $\varphi_K(J^{p^m}) = I_n$. If λ is an eigenvalue of $\varphi_K(J)$ then λ^{p^m} is an eigenvalue of $\varphi_K(J^{p^m})$, and so $\lambda^{p^m} = 1$ which implies that $\lambda = 1$. So, just as above, we can find invertible matrices $X_1, X_2, \ldots, X_s$ with entries in $\mathrm{GF}(p)$ such that $X_i^{-1}E_iX_i$ is in Jordan form (with 1 as the only eigenvalue) for $i = 1, 2, \ldots, s$. This gives the Jordan form of $\varphi_K(A)$ for all fields of characteristic p.

http://dx.doi.org/10.22108/ijgt.2018.112574.1498

It might be helpful to give a simple example. Let K be a field and let $A = aJ_2 \oplus bJ_3$ for some $a, b \in K$. If the characteristic of K is 0 or is a prime $p > 3$ then the Jordan form of $A \otimes A$ is

$$a^2J_1 \oplus a^2J_3 \oplus abJ_2 \oplus abJ_2 \oplus abJ_4 \oplus abJ_4 \oplus b^2J_1 \oplus b^2J_3 \oplus b^2J_5.$$

The exceptional characteristics are $p = 2, 3$. In characteristic 2 the Jordan form of $A \otimes A$ is

$$a^2J_2 \oplus a^2J_2 \oplus abJ_2 \oplus abJ_2 \oplus abJ_4 \oplus abJ_4 \oplus b^2J_1 \oplus b^2J_4 \oplus b^2J_4,$$

and in characteristic 3 it is

$$a^2J_1 \oplus a^2J_3 \oplus abJ_3 \oplus abJ_3 \oplus abJ_3 \oplus abJ_3 \oplus b^2J_3 \oplus b^2J_3 \oplus b^2J_3.$$

This example illustrates that it is much easier in practice than in theory to show for a given characteristic that when A is of form (5.1) then the Jordan form of $\varphi(A)$ depends only on the integers $k_1, k_2, \ldots, k_r$ and on the values of $\lambda_1, \lambda_2, \ldots, \lambda_r$. There are only finitely many possible choices for $k_1, k_2, \ldots, k_r$ which sum to m. For each such choice we treat the eigenvalues $\lambda_1, \lambda_2, \ldots, \lambda_r$ as indeterminates and compute the Jordan form of $\varphi(A)$ in characteristic zero. We then identify the exceptional characteristics, and compute the Jordan form in each exceptional characteristic.

Note that this example also covers the case when $a = b$ (in which case $A \otimes A$ has only 1 eigenvalue) and the case $a = -b$ (when $A \otimes A$ has two eigenvalues). In all other cases $A \otimes A$ has three eigenvalues.

6. The type of a matrix in GL(m, K)

Let K be a field, and let A be a matrix in $\mathrm{GL}(m, K)$. Let the primary invariant factors of A be $p_1(x)^{e_1}, p_2(x)^{e_2}, \ldots, p_k(x)^{e_k}$ where $p_1, p_2, \ldots, p_k$ are monic irreducible polynomials in $K[x]$. Let the distinct irreducible polynomials which occur in the sequence $p_1, p_2, \ldots, p_k$ be $q_1, q_2, \ldots, q_t$ (with $t \leq k$). For $1 \leq i \leq t$ let S_i be the multiset of exponents e such that q_i^e is one of the primary invariant factors of A. Then the type of A is the multiset of ordered pairs

$$\{(\deg q_1, S_1), (\deg q_2, S_2), \ldots, (\deg q_t, S_t)\}.$$

For example, if the primary invariant factors of A are $p(x)^2$, $p(x)^3$, $q(x)$, $q(x)$, $q(x)^4$ where p and q are distinct monic irreducible polynomials, then the type of A is

$$\{(\deg p, \{2, 3\}), (\deg q, \{1, 1, 4\})\}.$$

(Note that repeated entries in these multisets are significant.) So the type of A records the degrees of the different irreducible polynomials which arise in the primary invariant factors of A, together with the multiset of exponents associated with each of these irreducible polynomials. There are only finitely many possible types of matrices in $\mathrm{GL}(m, K)$. In addition if K has order q then the number of matrices in $\mathrm{GL}(m, K)$ of a given type is a polynomial in q. Green [3] proves that the size of the conjugacy class of A is a polynomial in q, with the polynomial depending only on the type of A. A formula for this polynomial is given on page 181 of [6].

If A is a matrix in Jordan form, and if A has the form (5.1), then the type of A depends only on which equalities $\lambda_i = \lambda_j$ $(i < j)$ hold between the eigenvalues of A. And for a given characteristic the type of $\varphi(A)$ depends only on which equalities $m_i = m_j$ $(i < j)$ hold between the eigenvalues of $\varphi(A)$. Thus in the example given at the end of the last section the type of A depends only on whether $a = b$ or not, and the type of $A \otimes A$ depends on whether $a = b$ or $a = -b$.

We want to use the results of Section 5 to compute the type of $\varphi(A)$ even when the characteristic polynomial of A does not split into linear factors, and we proceed as follows. Suppose that $A \in \mathrm{GL}(m, K)$ where K is a finite field of order q. Let L be the splitting field of the characteristic polynomial of A. Then let B be the Jordan form of A when considered as a matrix in $\mathrm{GL}(m, L)$. Suppose that $p(x)^e$ is a primary invariant factor of A, where $p(x)$ has degree d, and where λ is a root of $p(x)$ in L. Then the rational canonical form of A has the companion matrix of $p(x)^e$ as one of its blocks, and corresponding to this we have

$$\lambda J_e \oplus \lambda^q J_e \oplus \lambda^{q^2} J_e \oplus \cdots \oplus \lambda^{q^{d-1}} J_e$$

as a sum of blocks in B. Using the results of Section 5, the Jordan form of $\varphi_L(B)$ has the form

$$m_1 J_{t_1} \oplus m_2 J_{t_2} \oplus \cdots \oplus m_s J_{t_s}$$

for some positive integers $t_1, t_2, \ldots, t_s$, and some products $m_1, m_2, \ldots, m_s$ of the eigenvalues of B and their inverses. The integers $t_1, t_2, \ldots, t_s$ depend only on the type of A and the characteristic of K.

We need to investigate the eigenvalues of B and the products $m_1, \ldots, m_s$ more closely. Let the distinct irreducible polynomials which divide the primary invariant factors of A be $q_1, q_2, \ldots, q_t$, and let A have type

$$T = \{(n_1, S_1), (n_2, S_2), \ldots, (n_t, S_t)\},$$

where $n_i = \deg q_i$. We pick a root λ_i of the polynomial q_i for $i = 1, 2, \ldots, t$. Then the eigenvalues of B are $\{\lambda_i^{q^r} : 1 \le i \le t,\ 0 \le r < n_i\}$, and

$$B = \bigoplus_{i=1}^{t} \bigoplus_{j \in S_i} \bigoplus_{k=0}^{n_i - 1} \lambda_i^{q^k} J_j.$$

The eigenvalues λ_i satisfy the equations

$$\lambda_i^{q^{n_i}} = \lambda_i \ (i = 1, 2, \ldots, t). \tag{6.1}$$

They also satisfy the non-equations

$$\lambda_i^{q^r} \ne \lambda_i \ (0 < r < n_i,\ i = 1, 2, \ldots, t), \tag{6.2}$$

$$\lambda_i^{q^r} \ne \lambda_j^{q^s} \ (i \ne j,\ 0 \le r < n_i,\ 0 \le s < n_j). \tag{6.3}$$

The products $m_1, m_2, \ldots, m_s$ giving the eigenvalues of $\varphi_L(B)$ are of the form

$$\lambda_1^{h_1} \lambda_2^{h_2} \cdots \lambda_t^{h_t}$$

where $h_1, h_2, \ldots, h_t$ are integer polynomials in q. Note that these polynomials depend only on the type of A and on the characteristic of K. The map $m_i \longmapsto m_i^q$ gives a permutation of $m_1, m_2, \ldots, m_s$ and we can work out this permutation using the relations (6.1). Provided we know which relations $m_i = m_j$ hold for these particular values of $\lambda_1, \lambda_2, \ldots, \lambda_t$, and also know which of these relations do not hold, then we can work out the type of $\varphi_K(A)$. As we will see in Section 8, as well as being able to calculate the type of $\varphi_K(A)$ we also need to be able to calculate the dimension of the eigenspace of $\varphi_K(A)$ with eigenvalue 1. This is just the number of eigenvalues m_i $(1 \leq i \leq s)$ which are equal to 1 (for these particular values of $\lambda_1, \lambda_2, \ldots, \lambda_t$).

Now suppose that $\mu_1, \mu_2, \ldots, \mu_t \in L$ satisfy the relations (6.1) and the non-relations (6.2), (6.3). If we let g_i be the minimum polynomial of μ_i over K for $i = 1, 2, \ldots, t$ then

$$\bigoplus_{i=1}^{t} \bigoplus_{j \in S_i} \bigoplus_{k=0}^{n_i - 1} \mu_i^{q^k} J_j$$

is conjugate to matrices in $\mathrm{GL}(m, K)$ with primary invariant factors

$$\{g_i^j \,:\, 1 \leq i \leq t,\ j \in S_i\},$$

and all these matrices have type T. In this sense, $\mu_1, \mu_2, \ldots, \mu_t$ determines a conjugacy class of matrices of type T in $\mathrm{GL}(m, K)$. As we range over all possible solutions $\mu_1, \mu_2, \ldots, \mu_t$ the conjugacy classes determined by $\mu_1, \mu_2, \ldots, \mu_t$ range over all possible conjugacy classes of matrices of type T. Furthermore each such conjugacy class arises the same number of times. We get the same conjugacy class if we replace $\mu_1, \mu_2, \ldots, \mu_t$ by $\nu_1, \nu_2, \ldots, \nu_t$ where ν_i is conjugate to μ_i for all i. Also if $(n_i, S_i) = (n_j, S_j)$ then we obtain the same conjugacy class if we swap μ_i and μ_j. We can make this precise as follows. Write the entries (n_i, S_i) from T in a list

$$[(n_1, S_1), (n_2, S_2), \ldots, (n_t, S_t)]$$

and let G be the group of permutations π of $\{1, 2, \ldots, t\}$ such that

$$[(n_1, S_1), (n_2, S_2), \ldots, (n_t, S_t)] = [(n_{1\pi}, S_{1\pi}), (n_{2\pi}, S_{2\pi}), \ldots, (n_{t\pi}, S_{t\pi})].$$

Then as we range over all possible solutions in L of (6.1), (6.2) and (6.3) we run through all possible conjugacy classes of elements in $\mathrm{GL}(m, K)$ with type T, and each conjugacy class arises

$$n_1 n_2 \cdots n_t |G| \tag{6.4}$$

times.

To help clarify these ideas we investigate two simple examples. Let K be a finite field of order q, and let $A \in \mathrm{GL}(m, K)$ have primary invariant factors $g^2 h^3$ where g and h are different monic irreducible polynomials of degree 2. So A has type

$$\{(2, \{2\}), (2, \{3\})\}.$$

Let λ be a root of g and let μ be a root of h in the splitting field L of gh over K. Then the Jordan form of A over L is

$$B = \lambda J_2 \oplus \lambda^q J_2 \oplus \mu J_3 \oplus \mu^q J_3.$$

The eigenvalues of B satisfy $\lambda^{q^2} = \lambda$, $\mu^{q^2} = \mu$, $\lambda \neq \lambda^q$, $\mu \neq \mu^q$, $\lambda \neq \mu$, $\lambda \neq \mu^q$. These equalities and inequalities determine the type of A. (We also have inequalities $\lambda^q \neq \mu$, $\lambda^q \neq \mu^q$ but these are redundant.) We can run over all conjugacy classes of $\mathrm{GL}(m,K)$ of type $\{(2,\{2\}),(2,\{3\})\}$ by running over all possible choices of λ,μ in $\mathrm{GF}(q^2)$ satisfying these equations and non equations, and each conjugacy class will arise 4 times, since swapping λ and λ^q or μ and μ^q gives the same conjugacy class.

As a second example, suppose that K is a finite field of order q, and that $A \in \mathrm{GL}(m,K)$ has a single primary invariant factor g^3 where g is an irreducible quadratic. So A has type $\{2,\{3\}\}$. If we pick a root λ of g in $\mathrm{GF}(q^2)$ then the Jordan form of A when considered as a matrix over $\mathrm{GF}(q^2)$ is $\lambda J_3 \oplus \lambda^q J_3$. The eigenvalue λ satisfies $\lambda^{q^2} = \lambda$, $\lambda \neq \lambda^q$. Provided the characteristic of K is at least 5, the Jordan form of $A \otimes A$ over $\mathrm{GF}(q^2)$ is

$$\lambda^2 J_1 \oplus \lambda^2 J_3 \oplus \lambda^2 J_5 \oplus \lambda^{q+1} J_1 \oplus \lambda^{q+1} J_1 \oplus \lambda^{q+1} J_3$$
$$\oplus \lambda^{q+1} J_3 \oplus \lambda^{q+1} J_5 \oplus \lambda^{q+1} J_5 \oplus \lambda^{2q} J_1 \oplus \lambda^{2q} J_3 \oplus \lambda^{2q} J_5.$$

All the eigenvalues of $A \otimes A$ lie in the set $\{\lambda^2, \lambda^{q+1}, \lambda^{2q}\}$, and we have

$$(\lambda^2)^q = \lambda^{2q},\ (\lambda^{q+1})^q = \lambda^{q+1},\ (\lambda^{2q})^q = \lambda^2.$$

We also have

$$\lambda^2 \neq \lambda^{q+1},\ \lambda^{2q} \neq \lambda^{q+1},$$

so the type of $A \otimes A$ as a matrix over K depends on whether or not the equation $\lambda^2 = \lambda^{2q}$ is satisfied. So to compute the numbers of times matrices $A \otimes A$ of these two types arise as A ranges over conjugacy classes of type $\{2,\{3\}\}$ we need to count the numbers of choices of λ in $\mathrm{GF}(q^2)$ which satisfy the following two sets of equations and non-equations

$$\lambda^{q^2} = \lambda,\ \lambda \neq \lambda^q,\ \lambda^2 = \lambda^{2q},$$
$$\lambda^{q^2} = \lambda,\ \lambda \neq \lambda^q,\ \lambda^2 \neq \lambda^{2q}.$$

(We need to divide these answers by 2 to account for the fact that swapping λ and λ^q gives the same conjugacy class.) The dimension of the eigenspace of $A \otimes A$ with eigenvalue 1 is six if $\lambda^{q+1} = 1$, and zero otherwise.

7. Choosing elements from finite fields

Higman [5] proves the following theorem.

Theorem 7.1. *The number of ways of choosing a finite number of elements from $GF(q^n)$ subject to a finite number of monomial equations and inequalities between them and their conjugates over $GF(q)$, considered as a function of q, is PORC.*

Here we are choosing elements $x_1, x_2, \ldots, x_k$ (say) from the finite field $\mathrm{GF}(q^n)$ (where q is a prime power) subject to a finite set of equations and non-equations of the form

$$x_1^{n_1} x_2^{n_2} \cdots x_k^{n_k} = 1$$

and

$$x_1^{n_1} x_2^{n_2} \cdots x_k^{n_k} \neq 1$$

where $n_1, n_2, \ldots, n_k$ are integer polynomials in the Frobenius automorphism $x \to x^q$ of $\mathrm{GF}(q^n)$. Higman calls these equations and non-equations monomial. For example, as I showed in the first example at the end of Section 6, one way of computing the number of conjugacy classes of matrices $A \in \mathrm{GF}(q)$ of type $\{(2, \{2\}), (2, \{3\})\}$ is to count the number of choices of λ, μ in $\mathrm{GF}(q^2)$ satisfying

$$\lambda^{q^2} = \lambda,\ \mu^{q^2} = \mu,\ \lambda \neq \lambda^q,\ \mu \neq \mu^q,\ \lambda \neq \mu,\ \lambda \neq \mu^q,$$

and then divide by 4. Of course you can write these equations and non-equations as

$$\lambda^{q^2-1} = 1,\ \mu^{q^2-1} = 1,\ \lambda^{q-1} \neq 1,\ \mu^{q-1} \neq 1,\ \lambda\mu^{-1} \neq 1,\ \lambda\mu^{-q} \neq 1,$$

to match Higman's notation. Higman's proof of Theorem 7.1 involves 5 pages of homological algebra, but a shorter more elementary proof can be found in [8] and in [10].

To prove Theorem 7.1 you actually only need to prove that the number of ways of choosing a finite number of elements from $\mathrm{GF}(q^n)$ subject to a finite number of monomial equations between them and their conjugates over $\mathrm{GF}(q)$, considered as a function of q, is PORC. To see this suppose that we have a set S of equations and a set T of non-equations. Let T^* be the set of equations obtained from T be replacing all the $\neq$'s by $=$'s. For each subset $U \subseteq T^*$ let n_U be the number of solutions to the equations $S \cup U$. Then the number of solutions to the equations S and the non-equations T is

$$\sum_{U \subseteq T^*} (-1)^{|U|} n_U.$$

In [8] and in [10] I show that to find the number of ways of choosing a finite number of elements from $\mathrm{GF}(q^n)$ subject to a finite number of monomial equations S we write the equations in S as the rows of a matrix. We also have to add in equations $x_i^{q^n-1} = 1$ to make sure that the solutions lie in $\mathrm{GF}(q^n)$. For example, we represent the equations

$$x_1^{q^2-1} = 1,\ x_1^{q+1} x_2^{-2} = 1,\ x_1^{q^n-1} = 1,\ x_2^{q^n-1} = 1$$

by the matrix

$$\begin{bmatrix} q^2-1 & 0 \\ q+1 & -2 \\ q^n-1 & 0 \\ 0 & q^n-1 \end{bmatrix}.$$

For any given value of q this matrix is an integer matrix and the number of solutions to the equations is the product of the elementary divisors in the Smith normal form of the matrix. In [10] I show that the the number of solutions to a set of monomial equations, when considered as a function of q, is PORC. In fact I show that the number of solutions can be expressed in the form $df(q)$ for some primitive polynomial $f(x) \in \mathbb{Z}[x]$, where

$$d = \alpha + \sum_{i=1}^{r} \alpha_i \gcd(q - n_i, m_i)$$

for some rational numbers $\alpha, \alpha_1, \alpha_2, \ldots, \alpha_r$, some integers $m_1, m_2, \ldots, m_r$ with $m_i > 1$ for all i, and for some integers n_i with $0 < n_i < m_i$ for all i. In addition I give an algorithm for computing d and f.

8. Proof of Theorem 2.1

Let $\varphi : \mathrm{GL}(m, \mathbb{Q}) \to \mathrm{GL}(n, \mathbb{Q})$ give an algebraic family of groups, and let K be a finite field of order q, such that $\varphi_K(A)$ is defined for $A \in \mathrm{GL}(m, K)$. If we let V be a vector space of dimension n over K then we have a natural action of $\varphi_K(A)$ on V, and this gives an action of $\mathrm{GL}(m, K)$ on V. We want to prove that the number of orbits of $\mathrm{GL}(m, K)$ on V, when considered as a function of q, is PORC.

The number of orbits is given by Burnside's Lemma. It is

$$\frac{1}{|\mathrm{GL}(m, K)|} \sum_{A \in \mathrm{GL}(m,K)} \mathrm{fix}(\varphi_K(A)),$$

where $\mathrm{fix}(\varphi_K(A))$ is q^d where d is the dimension of the eigenspace of $\varphi_K(A)$ with eigenvalue 1. The number of orbits of $\mathrm{GL}(m, K)$ on k-dimensional subspaces of V is given by the same formula, where now $\mathrm{fix}(\varphi_K(A))$ is the number of k-dimensional subspaces W of V such that $W\varphi_K(A) = W$. So we need to show that the functions defined by these two formulae are PORC.

We simplify the problem as follows. There are only finitely many possible types for matrices $A \in \mathrm{GL}(m, K)$, and so it is sufficient to show that for each type T

$$\sum_{A \text{ has type } T} \mathrm{fix}(\varphi_K(A))$$

is PORC. Actually, there is a slight problem here since that would only show that the number of orbits had the form

$$\frac{f(q)}{|\mathrm{GL}(m, q)|}$$

for some PORC function f. However, as Higman observes in [5], if $k(x)$ is the quotient of two PORC functions, and if $k(x)$ only takes integral values, then $k(x)$ is PORC. This is because a rational function of x which takes integral values for infinitely many integral values of x is a polynomial.

Since the size of the conjugacy class of an element of type T in $\mathrm{GL}(m, q)$ is a polynomial in q which only depends on T, if we pick a set S_T of representatives for the conjugacy classes of type T then it is only necessary to show that

$$\sum_{A \in S_T} \mathrm{fix}(\varphi_K(A))$$

is PORC for each possible type T. As we saw in Section 6, if $A \in \mathrm{GL}(m,q)$ has type

$$T = \{(n_1, S_1), (n_2, S_2), \ldots, (n_t, S_t)\},$$

then the conjugacy class of A is determined by a set of eigenvalues $\lambda_1, \lambda_2, \ldots, \lambda_t$ satisfying the equations

$$\lambda_i^{q^{n_i}} = \lambda_i \ (i = 1, 2, \ldots, t), \tag{8.1}$$

and satisfying the non-equations

$$\lambda_i^{q^r} \neq \lambda_i \ (0 < r < n_i,\ i = 1, 2, \ldots, t), \tag{8.2}$$

$$\lambda_i^{q^r} \neq \lambda_j^{q^s} \ (i \neq j,\ 0 \leq r < n_i,\ 0 \leq s < n_j). \tag{8.3}$$

These eigenvalues can be taken to lie in $L = \mathrm{GF}(q^d)$ where d is the least common multiple of $\{n_1, n_2, \ldots, n_t\}$. As we run through all possible solutions to these equations and non-equations in L then the conjugacy classes in $\mathrm{GL}(m,K)$ determined by the solutions run through all conjugacy classes of elements of type T with each conjugacy class arising the same number of times. (This number is given by equation (6.4) from Section 6.) So it is sufficient to show that

$$\sum_{\lambda_1, \lambda_2, \ldots, \lambda_t} \mathrm{fix}(\varphi_K(A))$$

is PORC where now the sum runs over all solutions in L to the equations (8.1) and non-equations (8.2), (8.3), and where $A \in \mathrm{GL}(m,K)$ is chosen to lie in the conjugacy class determined by the solution.

So let $\lambda_1, \lambda_2, \ldots, \lambda_t$ satisfy the equations (8.1) and non-equations (8.2), (8.3). As we showed in Section 6, if A lies in the conjugacy class of $\mathrm{GL}(m,K)$ determined by $\lambda_1, \lambda_2, \ldots, \lambda_t$ then $\varphi_L(A)$ has Jordan normal form

$$m_1 J_{t_1} \oplus m_2 J_{t_2} \oplus \cdots \oplus m_s J_{t_s}$$

for some positive integers $t_1, t_2, \ldots, t_s$, and some products $m_1, m_2, \ldots, m_s$ of the form

$$\lambda_1^{h_1} \lambda_2^{h_2} \cdots \lambda_t^{h_t}$$

where $h_1, h_2, \ldots, h_t$ are integer polynomials in q. The integers $t_1, t_2, \ldots, t_s$ and the polynomials $h_1, h_2, \ldots, h_t$ depend only on the type T and the characteristic of K.

Now consider the proof of Theorem 2.1 (a). In this case, for any given solution $\lambda_1, \lambda_2, \ldots, \lambda_t$, $\mathrm{fix}(\varphi_K(A))$ is q^d where d is the number of equations $m_i = 1$ which are satisfied. The sequence $m_1, m_2, \ldots, m_s$ and the size of the Jordan block associated with each m_i depend on the characteristic as well as on the type T, so for the moment we assume that K has fixed characteristic p. For every subset $S \subseteq \{1, 2, \ldots, s\}$ let U_S be the set of equations $m_i = 1$ for $i \in S$ and let V_S be the set of non-equations $m_i \neq 1$ for $i \notin S$. Then Theorem 7.1 shows that the number of $\lambda_1, \lambda_2, \ldots, \lambda_t$ satisfying the equations and non-equations (8.1), (8.2), (8.3), U_S, V_S is PORC when considered as a function of q. For all the solutions $\mathrm{fix}(\varphi_K(A)) = q^{|S|}$. Every solution of (8.1), (8.2) and (8.3) satisfies (8.1), (8.2), (8.3), U_S, V_S for exactly one subset S, and so for each integer d the number of solutions to (8.1), (8.2)

http://dx.doi.org/10.22108/ijgt.2018.112574.1498

and (8.3) for which $\mathrm{fix}(\varphi_K(A)) = q^d$ is PORC, and hence for each characteristic p we obtain a PORC function $f_p(q)$ such that

$$\sum_{\lambda_1,\lambda_2,\ldots,\lambda_t} \mathrm{fix}(\varphi_K(A)) = f_p(q)$$

whenever q is a power of p. But as we saw in Section 5, there is a finite set of exceptional characteristics, and for all other characteristics the sequence $m_1, m_2, \ldots, m_s$ and the size of the Jordan block associated with each m_i depend only on T. So for each exceptional characteristic p we obtain a PORC function $f_p(q)$ giving

$$\sum_{\lambda_1,\lambda_2,\ldots,\lambda_t} \mathrm{fix}(\varphi_K(A))$$

when q is a power of p, and we obtain one further PORC function giving this sum for all other characteristics. It follows that

$$\sum_{\lambda_1,\lambda_2,\ldots,\lambda_t} \mathrm{fix}(\varphi_K(A))$$

is PORC as a function of q.

Finally consider the proof of Theorem 2.1 (b). Now $\mathrm{fix}(\varphi_K(A))$ is the number of k-dimensional subspaces W of V such that $W\varphi_K(A) = W$. Eick and O'Brien [1] show that this number is given by a polynomial in q, and that the polynomial only depends on the type of $\varphi_K(A)$. Furthermore they give an algorithm for computing this polynomial. As above, for the moment we assume that the characteristic of K is a fixed prime p. For any given solution $\lambda_1, \lambda_2, \ldots, \lambda_t$, the type of $\varphi_K(A)$ is determined by which equations $m_i = m_j$ hold (and which do not hold).

For every subset $S \subseteq \{(i, j) : 1 \leq i < j \leq s\}$ let U_S be the set of equations $m_i = m_j$ for $(i, j) \in S$ and let V_S be the set of non-equations $m_i \neq m_j$ for $(i, j) \notin S$. Then Theorem 7.1 shows that the number of $\lambda_1, \lambda_2, \ldots, \lambda_t$ satisfying the equations and non-equations (8.1), (8.2), (8.3), U_S, V_S is PORC when considered as a function of q. All the solutions to these equations give matrices $\varphi_K(A)$ of the same type, and every solution to (8.1), (8.2) and (8.3) satisfies (8.1), (8.2), (8.3), U_S, V_S for exactly one subset S. So for every possible type TT of $n \times n$ matrices, the number of solutions of (8.1), (8.2), (8.3) which give matrices $\varphi_K(A)$ of type TT is PORC, and hence for each characteristic p we obtain a PORC function $f_p(q)$ such that

$$\sum_{\lambda_1,\lambda_2,\ldots,\lambda_t} \mathrm{fix}(\varphi_K(A)) = f_p(q)$$

whenever q is a power of p.

The rest of the proof of Theorem 2.1 (b) follows in the same way as the proof of Theorem 2.1 (a).

It may help clarify the argument above if we look again at the example given at the end of Section 5. We were looking at the Jordan form of $A \otimes A$ when A has type $T = \{(1, \{2\}), (1, \{3\})\}$. Matrices $A = aJ_2 \oplus bJ_3$ where $a^{q-1} = 1$, $b^{q-1} = 1$, $a \neq b$ give a complete set of representatives for the conjugacy classes of matrices of type T over $\mathrm{GF}(q)$.

http://dx.doi.org/10.22108/ijgt.2018.112574.1498

If $q = p^k$ where $p > 3$ is prime then the Jordan form of the tensor square of $aJ_2 \oplus bJ_3$ is

$$a^2J_1 \oplus a^2J_3 \oplus abJ_2 \oplus abJ_2 \oplus abJ_4 \oplus abJ_4 \oplus b^2J_1 \oplus b^2J_3 \oplus b^2J_5.$$

So in the notation used above $s = 9$ and

$$(m_1, m_2, \ldots, m_9) = (a^2, a^2, ab, ab, ab, ab, b^2, b^2, b^2).$$

Since the sequence $m_1, m_2, \ldots, m_9$ has repetitions, many of the non-equations $m_i \neq m_j$ are impossible. Also since $a \neq b$ many of the equations $m_i = m_j$ are impossible. But this makes no difference to the argument above since the PORC formula giving the number of solutions to an impossible set of equations and non-equations will be 0. In our example $A \otimes A$ will have type

$$\{(1, \{1, 1, 3, 3, 5\}), (1, \{2, 2, 4, 4\})\}$$

if $a^2 = b^2$, and type

$$\{(1, \{1, 3\}), (1, \{2, 2, 4, 4\}), (1, \{1, 3, 5\})\}$$

if $a^2 \neq b^2$.

Similarly, to determine how may of $m_1, m_2, \ldots, m_9$ are equal to 1, we only need to determine which of a^2, ab, b^2 are equal to 1. If $a^2 = 1$ or if $b^2 = 1$ then $ab = 1$ is impossible, since $a \neq b$. So we need only compute the number of solutions to $a^{q-1} = 1$, $b^{q-1} = 1$, $a \neq b$ when combined with each of the following five sets of equations and non-equations:

$$a^2 = 1,\ ab \neq 1,\ b^2 = 1,$$

$$a^2 = 1,\ ab \neq 1,\ b^2 \neq 1,$$

$$a^2 \neq 1,\ ab \neq 1,\ b^2 = 1,$$

$$a^2 \neq 1,\ ab = 1,\ b^2 \neq 1,$$

$$a^2 \neq 1,\ ab \neq 1,\ b^2 \neq 1.$$

References

[1] B. Eick and E. A. O'Brien, Enumerating p-groups, *J. Austral. Math. Soc. Ser. A.*, **67** (1999) 191–205.

[2] B. Eick and M. Wesche, Enumeration of nilpotent associative algebras of class 2 over arbitrary fields, *J. Algebra*, **503** (2018) 573–589.

[3] J. A. Green, The characters of the finite general linear groups, *Trans. Amer. Math. Soc.*, **80** (1955) 402–447.

[4] G. Higman, Enumerating p-groups. I: Inequalities, *Proc. London Math. Soc.*, **10** (1960) 24–30.

[5] G. Higman, Enumerating p-groups. II: Problems whose solution is PORC, *Proc. London Math. Soc.*, **10** (1960) 566–582.

[6] I. G. Macdonald, *Symmetric functions and Hall polynomials*, The Clarendon Press, Oxford University Press, New York, 1979.

[7] M. F. Newman, E. A. O'Brien and M. R. Vaughan-Lee, Groups and nilpotent Lie rings whose order is the sixth power of a prime, *J. Algebra*, **278** (2004) 383–401.

[8] M. Vaughan-Lee, On Graham Higman's famous PORC paper, *Int. J. Group Theory*, **1** no. 4 (2012) 65–79.

http://dx.doi.org/10.22108/ijgt.2018.112574.1498

[9] M. Vaughan-Lee, Enumerating algbras over a finite field, *In. J. Group Theory*, **2** no. 3 (2013) 49–61.

[10] M. Vaughan-Lee, *Choosing elements from finite fields*, arXiv.1707.09652 (2017).

[11] B. Witty, *Enumeration of groups of prime-power order*, PhD thesis, Australian National University, 2006.

Michael Vaughan-Lee

Christ Church, Oxford, UK

Email: michael.vaughan-lee@chch.ox.ac.uk

http://dx.doi.org/10.22108/ijgt.2018.112574.1498