On Graham Higman's famous PORC paper

Michael Vaughan-Lee

February 2012

Abstract

We investigate Graham Higman's paper *Enumerating p-groups*, II, in which he formulated his famous PORC conjecture. We look at the possibilities for turning his theory into a practical algorithm for computing the number of p-class two groups of order p^n for small n. We obtain the PORC formulae for the number of r-generator groups of p-class two for $r \leq 6$. In addition, we obtain the PORC formula for the number of p-class two groups of order p^8.

One of the ideas used in implementing Higman's theory has led to a significant speed up in Eamonn O'Brien's ClassTwo function in MAGMA. In addition, we are able to simplify some of the theory. In particular, Higman's paper contains five pages of homological algebra which he uses in his proof that the number of solutions in a finite field to a finite set of *monomial* equations is PORC. It turns out that the homological algebra is just razzle dazzle, and can all be replaced by the single observation that if you write the equations as the rows of a matrix then the number of solutions is the product of the elementary divisors in the Smith normal form of the matrix.

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 [6] and [7]). In the first of these papers 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. Charles Sims improved the upper bound in 1965 (see [11]), proving that $f(p^n) \leq p^{\frac{2}{27}n^3+O(n^{\frac{8}{3}})}$. The best upper bound to date is due to Mike Newman and Craig Seeley: $f(p^n) \leq p^{\frac{2}{27}n^3+O(n^{\frac{5}{2}})}$. A proof of this bound can be found in the book *Enumeration of finite groups* [1] by Blackburn, Neumann and Venkataraman. These bounds on the number of p-groups of order p^n form a

critical ingredient in Laszlo Pyber's proof in [10] that the number of groups of order n is bounded by

$$n^{\frac{2}{27}\mu(n)^2+O(\mu(n)^{\frac{5}{3}})},$$

where $\mu(n)$ is the highest power to which any prime divides n. Using Newman and Seeley's upper bound, the error term in this theorem can be reduced to $\mathrm{O}(\mu(n)^{\frac{3}{2}})$. All these results are beautifully described in [1].

In the second of his two papers on enumerating p-groups Higman formulated his famous PORC conjecture concerning the form of the function $f(p^n)$ enumerating the number of p-groups of order 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 [9].) 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. The number of groups of order p^n is known to be PORC for $n \leq 7$, but Higman's conjecture remains open for $n \geq 8$. However Marcus du Sautoy and the current author have found a class two group G_p of order p^9 and exponent p with the property that the number of class 3 groups H of order p^{10} such that $H/\gamma_3(H) \cong G_p$ is not PORC. It may still be the case that $f(p^{10})$ *is* PORC, but this example does raise a strong possibility that Higman's conjecture fails for $n = 10$. The details of this example, and a history of the PORC conjecture can be found in [3].

In this article I am mainly concerned with Higman's proof in [7] that the number of p-class two groups of order p^n is PORC. (Higman uses the term Φ-class 2, meaning that the Frattini subgroup is central and of exponent p.) Actually Higman proves a much more general theorem than this about algebraic families of groups, and derives his result about the number of p-class two groups of order p^n as a corollary to this theorem. However this general theorem takes a page to state, and is stated in such generality that it is hard to see what is going on! Concentrating on the particular case of enumerating p-class two groups simplifies things considerably. In what follows below I shall describe how Higman's proof can be turned into a practical algorithm for computing the PORC formulae giving the number of p-class two groups of order p^n for small n. As far as I am aware, the only other work in this direction is in Brett Witty's Phd thesis [12], and I am very grateful to Brett for letting me have a copy of his thesis, and for a very helpful correspondence.

2 The p-groups of p-class two

Higman defines $g(r,s;p)$ to be the number of p-class two groups G of order p^{r+s} with $G/\Phi(G)$ elementary abelian of order p^r and with $\Phi(G)$ of order p^s. Higman calls these groups of Φ-complexion (r,s). Here $\Phi(G)$ is the Frattini subgroup of G, and since G has p-class two we have $\Phi(G)$ central and elementary abelian. We can describe

these groups as follows. First let P be the p-covering group of the elementary abelian p-group of rank r. This is the largest p-class two group with Frattini quotient of order p^r and it has Frattini subgroup $\Phi(P)$ of order $p^{\frac{1}{2}r(r+1)}$. The groups of Φ-complexion (r,s) are the quotient groups P/N, where N is a subgroup of $\Phi(P)$ of index p^s. If we think of the elementary abelian p-group of rank r as the additive group of the vector space V of dimension r over the field $\mathbb{F}_p$, then for $p>2$ we can think of $\Phi(P)$ as the additive group of the direct sum $V \oplus (V \wedge V)$, where $V \wedge V$ is the exterior square of V. The automorphism group of the elementary abelian group of rank r is $\mathrm{GL}(r,p)$, and this acts on V. Furthermore this action extends to an action on $V \oplus (V \wedge V)$, and two quotient groups P/M and P/N (with M and N subgroups of $V \oplus (V \wedge V)$) are isomorphic if and only if M and N are in the same orbit under this action. So, for $p>2$, $g(r,s;p)$ is the number of orbits of subspaces of codimension s in $V \oplus (V \wedge V)$ under the action of $\mathrm{GL}(r,p)$. This is Theorem 2.2 of [6]. A proof is also given in [1]. Note that by duality the number of orbits of subspaces of codimension s is the same as the number of orbits of subspaces of dimension s.

The subspaces of $V \oplus (V \wedge V)$ of dimension *at most* s correspond to $s \times \frac{1}{2}r(r+1)$ matrices over $\mathbb{F}_p$, with the rows of the matrices corresponding to elements of $V \oplus (V \wedge V)$. The group $\mathrm{GL}(r,p)$ acts on the right on these matrices, via its action on $V \oplus (V \wedge V)$, and the group $\mathrm{GL}(s,p)$ acts on the left. These $s \times \frac{1}{2}r(r+1)$ matrices over $\mathbb{F}_p$ correspond to subspaces of $V \oplus (V \wedge V)$ of dimension at most s, and two subspaces are in the same orbit under the action of $\mathrm{GL}(r,p)$ if and only if the corresponding matrices are in the same orbit under the action of $\mathrm{GL}(s,p) \times \mathrm{GL}(r,p)$. The number of these orbits is given by the Cauchy-Frobenius counting theorem, and is

$$\frac{1}{|\mathrm{GL}(s,p)| \cdot |\mathrm{GL}(r,p)|} \sum_h |\mathrm{fix}(h)|$$

where the sum is taken over all $h \in \mathrm{GL}(s,p) \times \mathrm{GL}(r,p)$, and $\mathrm{fix}(h)$ is the set of matrices fixed by h. We obtain the number of orbits of subspaces of dimension exactly s by subtracting the number of orbits of subspaces of dimension at most $s-1$ from the number of orbits of subspaces of dimension at most s.

Higman introduces a property of matrices called *type*, which he attributes to Green [5]. In Section 3 we show that if we take a fixed element $k \in \mathrm{GL}(r,p)$ then

$$\sum_{h \in \mathrm{GL}(s,p)} |\mathrm{fix}((h,k))|$$

is a polynomial in p, with the polynomial depending only on the type of the matrix giving the action of k on $V \oplus (V \wedge V)$. This does not help with Higman's proof that $g(r,s;p)$ is PORC, but it is a help with practical computation of $g(r,s;p)$. In particular, this result has been used to speed up Eamonn O'Brien's ClassTwo function in Magma [2], [4], which computes $g(r,s;p)$ for any given r,s,p.

3 The type of a matrix

The type of a square matrix describes the sizes of the blocks in the primary version of its rational canonical form. The rational canonical form of a matrix A is the matrix

$$\begin{bmatrix} C(p_1(x)^{e_1}) & 0 & 0 & 0 \\ 0 & C(p_2(x)^{e_2}) & 0 & 0 \\ 0 & 0 & \ddots & 0 \\ 0 & 0 & 0 & C(p_k(x)^{e_k}) \end{bmatrix},$$

with k blocks down the diagonal denoting the companion matrices of the primary invariant factors of A. These invariant factors are powers $p_i^{e_i}$ of monic irreducible polynomials $p_i(x)$. Let the distinct irreducible polynomials which occur in the rational canonical form of A be $q_1, q_2, \ldots, q_m$ (with $m \leq k$), and for $i = 1, 2, \ldots, m$ let S_i denote the multiset of exponents e such that q_i^e is an invariant factor of A. Then the type of A is the multiset of ordered pairs

$$\{(\deg q_1, S_1), (\deg q_2, S_2), \ldots, (\deg q_m, S_m)\}.$$

For example, if the primary invariant factors of A are $p(x)^2$, $p(x)^3$, $q(x)$, $q(x)$, $q(x)^4$ where $p(x)$ and $q(x)$ 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.) If $A \in \mathrm{GL}(n, p)$ then the number of conjugacy classes in $\mathrm{GL}(n, p)$ with the same type as A is a polynomial in p. Green [5] proves that the size of the conjugacy class of A is also a polynomial in p, with the polynomial depending only on the type of A. A formula for this polynomial is given on page 181 of [8]. (I found the formula, and the reference to [8] in Brett Witty's thesis [12].)

We now establish the result mentioned at the end of Section 2. Before stating the theorem, it may be helpful to set the context. For any given n there is a finite set of possible types for $n \times n$ matrices. For example, if $n = 2$ then there are four possible types:

$$\{(1, \{1, 1\})\},\ \{(1, \{2\})\},\ \{(1, \{1\}), (1, \{1\})\},\ \{(2, \{1\})\}.$$

Matrices of these four types are conjugate to matrices of the following forms:

$$\begin{bmatrix} \lambda & 0 \\ 0 & \lambda \end{bmatrix},\ \begin{bmatrix} \lambda & 1 \\ 0 & \lambda \end{bmatrix},\ \begin{bmatrix} \lambda & 0 \\ 0 & \mu \end{bmatrix},\ C(q(x)),$$

where $\lambda \neq \mu$ and where $q(x)$ is an irreducible quadratic. The number of conjugacy classes in $\mathrm{GL}(n, p)$ of any fixed type is given by a polynomial in p. So for $n = 2$ the number of conjugacy classes of each of these four types is

$$p - 1,\ p - 1,\ \frac{1}{2}(p-1)(p-2),\ \frac{1}{2}(p^2 - p).$$

Note that it is perfectly possible for these polynomials to evaluate to zero at particular values of p. For example, the third polynomial above evaluates to zero when $p = 2$.

Now let W be the space of $m \times n$ matrices over the field $\mathbb{F}_p$, and define an action of $\mathrm{GL}(m,p) \times \mathrm{GL}(n,p)$ on W as follows: if $M \in W$ and if $(A,B) \in \mathrm{GL}(m,p) \times \mathrm{GL}(n,p)$, then let M acted on by (A,B) be $A^{-1}MB$.

Theorem 1 *Let $B \in GL(n,p)$. Then*

$$\sum_{A \in GL(m,p)} |fix(A,B)|$$

is a polynomial in p depending only on the type of B.

Proof. Let T_n be the set of all possible types for $n \times n$ matrices. Then the theorem claims that for each $t \in T_n$ there is a polynomial $f_t(p)$ such that if $B \in \mathrm{GL}(n,p)$ has type t, then

$$\sum_{A \in \mathrm{GL}(m,p)} |\mathrm{fix}(A,B)| = f_t(p).$$

Let $(A,B) \in \mathrm{GL}(m,p) \times \mathrm{GL}(n,p)$. Then (A,B) acts as a linear transformation $S_{(A,B)}$ on W, and $\mathrm{fix}(A,B)$ is the eigenspace of $S_{(A,B)}$ corresponding to eigenvalue 1. The dimension of this eigenspace depends only on the conjugacy class of (A,B) in $\mathrm{GL}(m,p) \times \mathrm{GL}(n,p)$. Furthermore, the dimension of this eigenspace remains fixed even if we extend the ground field to include the eigenvalues of A^{-1} and B. So we can assume that $(A^{-1})^T$ and B are in Jordan canonical form. Let $(A^{-1})^T$ have Jordan blocks $J_1, J_2, \ldots, J_r$ and let B have Jordan blocks $K_1, K_2, \ldots, K_s$. Following Higman, we take our Jordan blocks to have a somewhat unusual form, with eigenvalues on the diagonal *and* on the superdiagonal. So the Jordan blocks look like

$$\begin{bmatrix} \lambda & \lambda & 0 & 0 \\ 0 & \lambda & \lambda & 0 \\ 0 & 0 & \lambda & \lambda \\ 0 & 0 & 0 & \lambda \end{bmatrix}.$$

This is possible since the eigenvalues are non-zero. Let A_i be the matrix obtained by replacing all the Jordan blocks in the Jordan form for $(A^{-1})^T$ by zeros, except for the i^{th} block. So

$$A_i = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & \ddots & 0 & 0 & 0 \\ 0 & 0 & J_i & 0 & 0 \\ 0 & 0 & 0 & \ddots & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix},$$

and $(A^{-1})^T = A_1 + A_2 + \ldots + A_r$. Similarly we write $B = B_1 + B_2 + \ldots + B_s$ where $B_1, B_2, \ldots, B_s$ are matrices corresponding to the Jordan blocks of B. Note that $A_i A_j = B_i B_j = 0$ for all $i \neq j$. For each i, j the subspace $A_i^T W B_j$ of W is

invariant under the action of (A, B), and W is the direct sum of these subspaces. If the Jordan block J_i corresponds to rows $u+1, u+2, \ldots, u+d$, and the Jordan block K_j corresponds to columns $v+1, v+2, \ldots, v+e$, then the subspace $A_i^T W B_j$ consists of the matrices which have zero entry in position (a, b) unless $u < a \leq u+d$ and $v < b \leq v+e$. We take a basis $\{E_{ab} \mid 1 \leq a \leq d,\ 1 \leq b \leq e\}$ for this subspace, where E_{ab} is the matrix in W with all entries zero, except for a 1 in position $(u+a, v+b)$. Let λ be the eigenvalue of the block J_i and let μ be the eigenvalue of the block K_j. Then the action of (A, B) on these basis elements is as follows:

$$\begin{aligned}
E_{ij} &\mapsto \lambda\mu(E_{ij} + E_{i\,j+1} + E_{i+1\,j} + E_{i+1\,j+1}) \text{ if } i < d \text{ and } j < e,\\
E_{ie} &\mapsto \lambda\mu(E_{ie} + E_{i+1\,e}) \text{ if } i < d,\\
E_{dj} &\mapsto \lambda\mu(E_{dj} + E_{d\,j+1}) \text{ if } j < e,\\
E_{de} &\mapsto \lambda\mu E_{de}.
\end{aligned}$$

So (A, B) has a single eigenvalue $\lambda\mu$ in its action on $A_i^T W B_j$. Higman's trick of taking eigenvalues along the superdiagonal makes it clear that the dimension of the corresponding eigenspace is independent of the particular values of λ and μ, and it is not hard to see that this dimension is $\min(d, e)$. So the dimensions of the various eigenspaces depend only on the sizes of the Jordan blocks, and not on the particular eigenvalues, or the particular prime. However there is a trap here for the unwary. The Jordan form of the action of (A, B) on the subspace $A_i^T W B_j$ *does* depend on the prime. The number of Jordan blocks is the dimension of the eigenspace, and this is independent of p, but the sizes of the blocks do depend on p. For example, if we take $d = e = 2$, then the subspace has dimension 4. When $p = 2$ we have two 2×2 Jordan blocks, and when $p > 2$ we have one 3×3 block and one 1×1 block. We will return to this issue in Section 4.

We return to the problem of determining the dimension of the eigenspace of $S_{(A,B)}$ corresponding to eigenvalue 1. Since the eigenvalues of A^{-1} are the inverses of the eigenvalues of A, we see that 1 can only be an eigenvalue of $S_{(A,B)}$ if A and B have an eigenvalue in common. Let the irreducible polynomials involved in the invariant factors of B (over $\mathbb{F}_p$) be $q_1, q_2, \ldots, q_c$. Then A can only have an eigenvalue in common with B if at least one of its invariant factors involves a polynomial from the set $\{q_1, q_2, \ldots, q_c\}$. Fix the type of A, and consider the possible choices of primary invariant factors for all the different A of that type. If none of the primary invariant factors of A involve polynomials in the set $\{q_1, q_2, \ldots, q_c\}$ then the dimension of the eigenspace of $S_{(A,B)}$ corresponding to eigenvalue 1 is zero. Suppose however that A has primary invariant factors involving q_1, and let these factors be $q_1^{e_1}, q_1^{e_2}, \ldots, q_1^{e_a}$. (Note that this is only possible if the type of A contains $(\deg q_1, \{e_1, e_2, \ldots, e_a\})$.) Let q_1 have degree k, and let the roots of q_1 in the field of p^k elements be $\lambda_1, \lambda_2, \ldots, \lambda_k$. Then for each $i = 1, 2, \ldots, k$ the Jordan canonical form of $(A^{-1})^T$ contains Jordan blocks of size $e_1, e_2, \ldots, e_a$ with eigenvalue λ_i^{-1}. Let the primary invariant factors of B involving q_1 be $q_1^{f_1}, q_1^{f_2}, \ldots, q_1^{f_b}$, so that the Jordan canonical form of B contains Jordan blocks of size $f_1, f_2, \ldots, f_b$ with eigenvalue λ_i for $i = 1, 2, \ldots, k$. Then the calculation in the paragraph above shows that the primary invariant factors in A and

B involving q_1 contribute

$$k \sum_{1 \le i \le a,\, 1 \le j \le b} \min(e_i, f_j)$$

to the dimension of the eigenspace of $S_{(A,B)}$ corresponding to eigenvalue 1. We obtain similar formulae for the contributions to the dimension of this eigenspace arising from the primary invariant factors in A and B invoving $q_2, q_3, \ldots, q_c$. For each $i = 1, 2, \ldots, c$ let E_i be the multiset of exponents e such that q_i^e is a primary invariant factor of A, and let F_i be the multiset of exponents e such that q_i^e is a primary invariant factor of B. (Some, or all, of the multisets E_i may be empty.) Then the dimension of the eigenspace of $S_{(A,B)}$ corresponding to eigenvalue 1 depends only on the multisets E_i and F_i $(1 \le i \le c)$ and on the degrees of $q_1, q_2, \ldots, q_c$. The dimension of the eigenspace does not depend on the particular prime p or on the particular choice of $q_1, q_2, \ldots, q_c$. If A has type t then a particular choice of $E_1, E_2, \ldots, E_c$ is only possible if the multiset $\{(\deg q_i, E_i) \,|\, 1 \le i \le c,\, E_i \ne \varnothing\}$ is contained in t. So for any given t there are only finitely many choices for $E_1, E_2, \ldots, E_c$. Furthermore, for each t and each possible choice of $E_1, E_2, \ldots, E_c$, the number of ways of choosing the remaining invariant factors of A so that A has type t is given by a polynomial in p. The conjugacy classes of type t all have the same size, and this size is given by a polynomial in p. So the number of times each possible dimension of $\mathrm{fix}(A, B)$ arises as A ranges over all matrices of type t is a polynomial in p. This implies that if we sum $|\mathrm{fix}(A, B)|$ over all A of type t then we obtain a polynomial in p. Since there are only finitely many possible types t for A we see that

$$\sum_{A \in \mathrm{GL}(m,p)} |\mathrm{fix}(A, B)|$$

is a polynomial in p. None of the calculations above depend on the choice of $q_1, q_2, \ldots, q_c$, but only on their degrees, so this polynomial in p depends only on the type of B. □

4 Computing the action on $V \oplus (V \wedge V)$

If $A \in \mathrm{GL}(r, p)$ we need to be able to compute the matrix B giving the action of A on $V \oplus (V \wedge V)$, and we need to be able to compute the number of B of each type. (This is so we can use Theorem 1.) Actually, B takes the form

$$\begin{bmatrix} A & 0 \\ 0 & C \end{bmatrix},$$

where C gives the action of A on $V \wedge V$, so the problem is to compute C. To illustrate the issues that arise, it is sufficient to consider the case when A is in Jordan canonical form. If A is diagonal with eigenvalues $\lambda_1, \lambda_2, \ldots, \lambda_r$ then C is diagonal with eigenvalues $\lambda_i \lambda_j$ with $1 \le i < j \le r$, which is straightforward. But things are

more complicated when A is not diagonal. An example will be sufficient to illustrate the problem.

Let

$$A = \begin{bmatrix} \lambda & \lambda & 0 & 0 \\ 0 & \lambda & \lambda & 0 \\ 0 & 0 & \lambda & \lambda \\ 0 & 0 & 0 & \lambda \end{bmatrix},$$

and we suppose that A is the matrix of a linear transformation $\alpha : V \to V$ with respect to a basis v_1, v_2, v_3, v_4 for V. Then taking a basis $v_1 \wedge v_2$, $v_1 \wedge v_3$, $v_1 \wedge v_4$, $v_2 \wedge v_3$, $v_2 \wedge v_4$, $v_3 \wedge v_4$ for $V \wedge V$ we see that

$$C = \lambda^2 \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

If you treat C as a matrix over a field of characteristic zero then the Jordan canonical form of C is

$$\lambda^2 \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix},$$

but the determinant of the matrix which transforms C into Jordan canonical form is 8. (Or at least one of the transforming matrices has determinant 8.) The transforming matrix is an integer matrix, and so this implies that the Jordan canonical form of C over $\mathbb{F}_p$ is as above, provided $p > 2$. When $p = 2$, the Jordan form is

$$\lambda^2 \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

More generally, if A is in Jordan canonical form, then the matrix C will have a sequence of square blocks down the diagonal, and zeros elsewhere. Each block will have the form $\lambda\mu D$, where λ and μ are eigenvalues of A and where D is a matrix with entries 0 and 1 and all eigenvalues equal to 1. (With a natural choice of basis, D will be an upper triangular matrix, with 1's down the diagonal.) If you treat D as a matrix over the rationals, then you can compute its Jordan canonical form. The transforming matrix will be a matrix with rational entries, and rational determinant

$\frac{m}{n}$. So this computation of the Jordan form of D will be valid over $\mathbb{F}_p$ provided p does not divide m or n, and provided p does not divide any of the denominators of the coefficients of the transforming matrix. In this way we are able to compute the Jordan form of C for all but a finite set of primes. If required, we can then go back and recompute the Jordan form of C for the exceptional primes. Higman only needed to know that there were only finitely many exceptional primes, but for practical computation we need to know which primes are exceptional.

Once we know the Jordan form of C, and hence the Jordan form of the matrix B giving the action of A on $V \oplus (V \wedge V)$, we still need to compute the type of B. Consider the following example to illustrate the problem.

Let A be a diagonal matrix in $\mathrm{GL}(3,p)$ with eigenvalues a, b, c. Then B is a diagonal matrix with eigenvalues a, b, c, ab, ac, bc. The type of B depends on which of these 6 eigenvalues are equal and which are not equal. Some of the possible equalities can be simplified — for instance $a = ab$ is equivalent to $b = 1$. And some of the possible equalities are equivalent to each other — for instance $ab = ac$ is equivalent to $b = c$. After simplification, and after removing duplicates, we are left with 9 possible equations:

$$a = b,\ a = c,\ b = c,\ a = 1,\ b = 1,\ c = 1,\ a = bc,\ b = ac,\ c = ab.$$

The type of B is determined by which of these equations hold, and which do not hold. (Since $a, b, c \in \mathbb{F}_p \backslash \{0\}$, they also satisfy the equations $a^{p-1} = 1$, $b^{p-1} = 1$, $c^{p-1} = 1$.) We will show in Section 5 below how to compute the number of choices for $a, b, c \in \mathbb{F}_p \backslash \{0\}$ subject to satisfying a subset of these equations. If S is a subset of the equations let $f(S)$ denote the number of possible solutions for a, b, c subject to satisfying the equations in S *and possibly some of the other equations as well.* Then the number of solutions for a, b, c satisfying the equations in S *and no others* is

$$\sum_{S \subseteq T} (-1)^{|T \backslash S|} f(T),$$

where the sum is taken over all possible subsets T of the 9 equations satisfying $T \supseteq S$. In this way we are able to calculate the number of B of each type, as a, b, c range over $\mathbb{F}_p \backslash \{0\}$.

As a second example, consider a matrix $A \in \mathrm{GL}(3,p)$ with one invariant factor of degree 1 and one which is irreducible of degree 2. Let the root of the degree one polynomial be $a \in \mathbb{F}_p$, and let $b, b^p \in \mathbb{F}_{p^2}$ be the roots of the quadratic. Then the eigenvalues of A are a, b, b^p. These eigenvalues satisfy $a^{p-1} = 1$, $b^{p^2-1} = 1$, $b^{p-1} \neq 1$. The matrix B is semisimple, with eigenvalues $a, b, b^p, b^{p+1}, ab, ab^p$. Note that $b^{p+1} \in \mathbb{F}_p$, but that ab and ab^p are roots of an irreducible quadratic. To know the type of B we need to know whether the equation $a = b^{p+1}$ is satisfied or not. In addition, we need to know whether the eigenvalues b, b^p are roots of the same irreducible quadratic as the eigenvalues ab, ab^p. This will be the case if $a = 1$ or if $b = ab^p$. So we have a total of 6 equations, and the type of B is determined by which of the 6 equations are satisfied, and which are not satisfied.

As a final example, let $A \in \mathrm{GL}(4,p)$ have a single invariant factor which is irreducible of degree 4. If a is a root of this polynomial then the eigenvalues of A are a, a^p, a^{p^2}, a^{p^3} with $a^{p^4-1} = 1$ and $a^{p^2-1} \neq 1$. The matrix B is semisimple with eigenvalues

$$a, a^p, a^{p^2}, a^{p^3}, a^{p+1}, a^{p^2+1}, a^{p^3+1}, a^{p^2+p}, a^{p^3+p}, a^{p^3+p^2}.$$

The eigenvalues $a^{p+1}, a^{p^2+p}, a^{p^3+p^2}, a^{p^3+1}$ are roots of a quartic which is irreducible unless $a^{p^3+p^2-p-1} = 1$, in which case it reduces to the square of a quadratic. The eigenvalues a^{p^2+1}, a^{p^3+p} are roots of a quadratic, which reduces to the square of a degree one polynomial if $a^{p^3-p^2+p-1} = 1$. The two quartic polynomials are identical if $a^{p^2+p-1} = 1$ or $a^{p^3+p^2-1} = 1$. Finally, we have to consider the possibility that a^{p^2+1} equals one of $a^{p+1}, a^{p^2+p}, a^{p^3+p^2}, a^{p^3+1}$, but a little thought shows that this is impossible. So we have a total of 6 equations, and the type of B is determined by which of the 6 equations are satisfied, and which are not satisfied.

5 Choosing elements from finite fields

As we saw in Section 4, to compute the number of matrices of each type in the action of $\mathrm{GL}(r,p)$ on $V \oplus (V \wedge V)$, we need to be able to find the number of solutions to various sets of equations. The trick is to write the relevant equations as the rows of a matrix.

Consider the first example above, and suppose we want to find how many a, b, c there are in $\mathbb{F}_p \backslash \{0\}$ satisfying the relations $a = bc$ and $b = ac$. We need to add in the relations $a^{p-1} = 1$, $b^{p-1} = 1$, $c^{p-1} = 1$, and then we have the matrix

$$\begin{bmatrix} p-1 & 0 & 0 \\ 0 & p-1 & 0 \\ 0 & 0 & p-1 \\ -1 & 1 & 1 \\ 1 & -1 & 1 \end{bmatrix}.$$

In the second example, suppose that we want to find how many elements a and b there are in $\mathbb{F}_{p^2}$ satisfying the relations $a^{p-1} = 1$, $b^{p^2-1} = 1$, $b = ab^p$. Then we consider the matrix

$$\begin{bmatrix} p-1 & 0 \\ 0 & p^2-1 \\ 1 & p-1 \end{bmatrix}.$$

(Note that the solutions to these equations will include solutions in which $b \in \mathbb{F}_p$, and we will need to exclude them by also considering how many solutions there are to the equations $a^{p-1} = 1$, $b^{p-1} = 1$, $b = ab^p$.)

We now show how to use these matrices to compute the number of solutions to the equations they encode. First consider the case when p is a given prime, so that we have an integer matrix. We will show in a moment that in this case the number of solutions to the equations is the product of the elementary divisors in the Smith normal form of the matrix. So consider the case when the prime p is symbolic. Then

the entries in the matrix are integer polynomials in p. The matrix will have rank k where k is the number of columns in the matrix, and the product of the elementary divisors in the Smith normal form is the greatest common divisor of the $k \times k$ minors of the matrix. These minors are integer polynomials in the prime p, and the greatest common divisor of a set of integer polynomials in p is PORC. To see this, consider the greatest common divisor of a set $f_1, f_2, \ldots, f_r$ of integer polynomials in p. Treat these polynomials as polynomials with rational coefficients, and use the Euclidean algorithm to compute their greatest common divisor over $\mathbb{Q}$. We can take this to be a primitive integer polynomial f, and we obtain rational polynomials $g_1, g_2, \ldots, g_r$ such that

$$g_1 f_1 + g_2 f_2 + \ldots + g_r f_r = f.$$

If we let m be the least common multiple of the denominators of the coefficients in the polynomials $g_1, g_2, \ldots, g_r$, then we see that for any given prime p the greatest common divisor of $f_1(p), f_2(p), \ldots, f_r(p)$ over $\mathbb{Z}$ is $nf(p)$ for some n dividing m. The value of n will depend on the residue class of p modulo m, and it is straightforward to compute the value of n for each residue class. Of course this value might be the same, n say, for each residue class in which case the greatest common divisor of $f_1(p), f_2(p), \ldots, f_r(p)$ over $\mathbb{Z}$ is $nf(p)$ for all primes p. In particular, if $m = 1$ then the greatest common divisor of $f_1(p), f_2(p), \ldots, f_r(p)$ over $\mathbb{Z}$ is $f(p)$ for all primes p. In the case when $m > 1$, and when the value of n is not the same for each residue class, then it is not hard to see that we can express the value of n in the form

$$\alpha + \sum_{i=1}^{k} \alpha_i \gcd(p - a_i, m_i),$$

where $\alpha \in \mathbb{Q}$ and where for each $1 \leq i \leq k$ we have $\alpha_i \in \mathbb{Q}$, $m_i | m$, $m_i \neq 1$, $0 < a_i < m_i$.

It remains to show that if p is a given prime, so that the matrix is an integer matrix, then the number of solutions to the equations is the product of the elementary divisors in the Smith normal form of the matrix. Let A be one of these relation matrices, and suppose it has k columns corresponding to elements $a_1, a_2, \ldots, a_k$ in the multiplicative group of the field of order p^n. (Some of the equations may specify that some of the elements lie in subfields, but this does not matter.) Let ω be a primitive element in $\mathbb{F}_{p^n}$, and write $a_i = \omega^{m_i}$ for $i = 1, 2, \ldots, k$, taking the exponents m_i as elements in $\mathbb{Z}_{p^n-1}$. Then a row $(\beta_1, \beta_2, \ldots, \beta_k)$ in the matrix A corresponds to a relation $\beta_1 m_1 + \beta_2 m_2 + \ldots + \beta_k m_k = 0$ which we require the exponents to satisfy. The matrix A can be reduced to Smith normal form by elementary row and column operations. As we apply these operations, the relations encoded in the matrix change. But we show that at each step the number of solutions to the relations stays constant.

This is clear for elementary row operations, since an elementary row operation replaces the relations by an equivalent set of relations. So we need to consider the effect of elementary column operations. We can consider the k-tuples $(m_1, m_2, \ldots, m_k)$ as elements in the additive group $G = \mathbb{Z}_{p^n-1} \times \mathbb{Z}_{p^n-1} \times \ldots \times \mathbb{Z}_{p^n-1}$. Let A be one of these relation matrices, and let B be the matrix obtained from A after applying an

elementary column operation. For each such operation we define an automorphism σ of G with the property that $g \in G$ satisfies the relations given by the rows of A if and only if $g\sigma$ satisfies the relations given by the rows of B. This shows that the number of elements in G satisfying the relations given by A is the same as the number of elements in G satisfying the relations given by B. If the elementary column operation swaps two columns of A then we let σ be the automorphism which swaps the corresponding entries in $(m_1, m_2, \ldots, m_k)$, and if the elementary column operation multiplies a column by -1 we let σ be the automorphism which multiplies the corresponding entry in $(m_1, m_2, \ldots, m_k)$ by -1. Finally, if the elementary column operation subtracts α times column j from column i, then we let σ be the automorphism which leaves all the entries in $(m_1, m_2, \ldots, m_k)$ fixed except for the j-th entry, which it replaces by $m_j + \alpha m_i$.

The argument above shows that the number of $g \in G$ satisfying the original set of relations given by the rows of A is the same as the number of $g \in G$ satisfying the relations given by the Smith normal form A. If the elementary divisors in the Smith normal form are $d_1, d_2, \ldots, d_k$, then $(m_1, m_2, \ldots, m_k)$ is a solution to these equations if and only if

$$d_1 m_1 = d_2 m_2 = \ldots = d_k m_k = 0.$$

Provided we can show that $d_i | p^n - 1$ for all i, this shows that the number of solutions is $d_1 d_2 \ldots d_k$, as claimed.

If A is one of these relation matrices with k columns, then the rows of A are elements in the free $\mathbb{Z}$-module $F = \mathbb{Z}^k$. We let $R(A)$ denote the $\mathbb{Z}$-submodule of F generated by the rows of A. Our claim that $d_i | p^n - 1$ for all i amounts to the claim that $(p^n - 1)F \leq R(S)$, where S is the Smith normal form of our initial relation matrix. The Smith normal form is obtained from the initial matrix by a sequence of elementary row and column operations, and we show that $(p^n - 1)F \leq R(B)$ for all the matrices B generated in this sequence.

Let A be the starting matrix. Then it contains rows

$$(p^{n_1} - 1, 0, 0, \ldots, 0),\ (0, p^{n_2} - 1, 0, \ldots, 0),\ \ldots,\ (0, 0, \ldots, 0, p^{n_k} - 1)$$

for some $n_1, n_2, \ldots, n_k$ dividing n. So it is clear that $(p^n - 1)F \leq R(A)$. Suppose that at some intermediate stage in the reduction of A to Smith normal form we have two matrices B and C, where C is obtained from B by an elementary row operation or an elementary column operation. We assume by induction that $(p^n - 1)F \leq R(B)$, and we show that this implies that $(p^n - 1)F \leq R(C)$. This is clear if C is obtained from B by an elementary row operation, since then $R(B) = R(C)$. So consider the case when C is obtained from B by an elementary column operation. This column operation corresponds to an automorphism σ of F, and if r is a row of B then the corresponding row of C is $r\sigma$. So $R(C) = R(B)\sigma$, and the fact that $(p^n - 1)F$ is a characteristic submodule of F implies that $(p^n - 1)F \leq R(C)$.

This completes the proof that the number of solutions to the relations given by the rows of the matrix is equal to the product of the elementary divisors in the Smith normal form.

6 The method

As we have seen, if A is a matrix of a given type then we can write down a set of monomial equations which the eigenvalues of A satisfy, and a further set of monomial equations which they do not satisfy. For example, if A is a 3×3 matrix with type $\{(1,\{1\}),(2,\{1\})\}$ then A has one primary invariant factor of degree 1 and one of degree 2. The eigenvalues of A are a, b, b^p where $a^{p-1} = 1$, $b^{p^2-1} = 1$, $b^{p-1} \neq 1$. As we saw in Section 4, given the type of A we can compute the matrix $\begin{bmatrix} A & 0 \\ 0 & C \end{bmatrix}$ giving the action of A on $V \oplus (V \wedge V)$, expressing the eigenvalues of $\begin{bmatrix} A & 0 \\ 0 & C \end{bmatrix}$ in terms of the eigenvalues of A. We then obtain additional equations in the eigenvalues of $\begin{bmatrix} A & 0 \\ 0 & C \end{bmatrix}$, and the type of $\begin{bmatrix} A & 0 \\ 0 & C \end{bmatrix}$ is determined by which of these additional equations are satisfied and which are not satisfied. For each set of equations and non-equations we use the method described in Section 5 to determine the PORC formula for the number of solutions to the given equations and non-equations. In this way we are able to compute the PORC formula for the number of $\begin{bmatrix} A & 0 \\ 0 & C \end{bmatrix}$ of any given type as A ranges over $\mathrm{GL}(r,p)$. We then use Theorem 1 to compute $g(r,s;p)$.

There is a file named "porcprogs" on my website http://users.ox.ac.uk/~vlee/PORC/ which contains some MAGMA programs implementing Theorem 1.

7 Results

We have computed PORC formulae giving the values of $g(r,s;p)$ for $r = 1$, 2, 3, 4, 5, 6 (and all s). The values of $g(r,s;p)$ for $r = 1,2,3$ have already appeared in the literature, but most of the values for $r = 4,5,6$ are new. Most of these formulae have hundreds of terms, so it is not possible to list them all in this article. But I have placed a file named "grsps" containing them all on my website, and it can be found at http://users.ox.ac.uk/~vlee/PORC/. Here I give the values of $g(r,s;p)$ for $r+s \leq 8$. I also give the PORC formulae giving the number of p-class two groups of order p^k for $k \leq 8$. These formulae are already known for $k \leq 7$, but the formula for $k = 8$ is new.

Note that $g(r,s;p) = 0$ for $s > \frac{1}{2}r(r+1)$, and that $g(r,s;p) = 1$ for $s = \frac{1}{2}r(r+1)$. For $1 \leq s < \frac{1}{2}r(r+1)$ we have $g(r,s;p) = g(r,\frac{1}{2}r(r+1)-s;p)$. Higman's theory only works for odd primes, and so the formulae only apply for $p > 2$. The formulae $g(r,s;p)$ are valid for all $p > 2$ provided $r \leq 4$, but $p = 2,3,5$ are exceptional primes (as described in Section 4) for most of the formulae $g(5,s;p)$. The primes 2,3,5,7 are exceptional primes for most of the formulae $g(6,s;p)$. So the formulae $g(5,s;p)$ are only guaranteed correct for $p > 5$, and the formulae $g(6,s;p)$ are only guaranteed correct for $p > 7$. The "missing" values for small primes (including the prime 2) can easily be computed using Eamonn O'Brien's ClassTwo function in MAGMA [2], [4]. The command "ClassTwo(p,r,s);" will return $g(r,s;p)$ fairly promptly for moderate

values of r, s, p.

$$g(1,1;p) = 1$$

$$\begin{aligned} g(2,1;p) &= 3 \\ g(2,2;p) &= 3 \\ g(2,3;p) &= 1 \end{aligned}$$

$$\begin{aligned} g(3,1;p) &= 4 \\ g(3,2;p) &= p+14 \\ g(3,3;p) &= 3p+27 \\ g(3,4;p) &= p+14 \\ g(3,5;p) &= 4 \\ g(3,6;p) &= 1 \end{aligned}$$

$$\begin{aligned} g(4,1;p) &= 6 \\ g(4,2;p) &= 4p+48 \\ g(4,3;p) &= p^5+2p^4+7p^3+25p^2+88p+p\gcd(p-1,3)+\frac{9}{2}\gcd(p-1,3) \\ &\quad +\gcd(p-1,4)+\frac{1}{2}\gcd(p+1,3)+268 \\ g(4,4;p) &= p^8+2p^7+5p^6+10p^5+24p^4+53p^3+p^2\gcd(p-1,3)+138p^2 \\ &\quad +6p\gcd(p-1,3)+2p\gcd(p-1,4)+323p+21\gcd(p-1,3) \\ &\quad +6\gcd(p-1,4)+\frac{5}{4}\gcd(p-1,5)+2\gcd(p+1,3) \\ &\quad +\frac{1}{4}\gcd(p+1,5)+\frac{1}{4}\gcd(p^2+1,5)+\frac{2753}{4} \end{aligned}$$

$$\begin{aligned} g(5,1;p) &= 7 \\ g(5,2;p) &= p^2+15p+\frac{1}{2}\gcd(p-1,3)+\frac{1}{2}\gcd(p+1,3)+123 \\ g(5,3;p) &= p^{11}+2p^{10}+5p^9+10p^8+20p^7+38p^6+74p^5+142p^4+p^3\gcd(p-1,3) \\ &\quad +277p^3+8p^2\gcd(p-1,3)+2p^2\gcd(p-1,4)+558p^2 \\ &\quad +30p\gcd(p-1,3)+11p\gcd(p-1,4)+p\gcd(p-1,5)+1120p \\ &\quad +67\gcd(p-1,3)+29\gcd(p-1,4)+3\gcd(p-1,5)+2010 \end{aligned}$$

$$\begin{aligned} g(6,1;p) &= 9 \\ g(6,2;p) &= p^3+7p^2+53p+2\gcd(p-1,3)+316 \end{aligned}$$

$$g(7,1;p)=10$$

The numbers of p-class two groups of order p^2, p^3 and p^4 are 1, 3 and 7 respectively, and these numbers are valid for all primes p. For odd primes p the numbers of groups of p-class two of order p^5, p^6 and p^7 are respectively $p+21$, $7p+82$ and

$$\begin{aligned} &p^5+2p^4+7p^3+26p^2+p\gcd(p-1,3)+104p+5\gcd(p-1,3) \\ &+\gcd(p-1,4)+\gcd(p+1,3)+414. \end{aligned}$$

And finally, for $p>3$ the number of p-class two groups of order p^8 is

$$\begin{aligned} &p^{11}+2p^{10}+5p^9+11p^8+22p^7+43p^6+84p^5+166p^4+p^3\gcd(p-1,3)+331p^3 \\ &+9p^2\gcd(p-1,3)+2p^2\gcd(p-1,4)+703p^2+36p\gcd(p-1,3) \\ &+13p\gcd(p-1,4)+p\gcd(p-1,5)+1496p+88\gcd(p-1,3)+35\gcd(p-1,4) \\ &+\frac{17}{4}\gcd(p-1,5)+\frac{1}{4}\gcd(p+1,5)+\frac{1}{4}\gcd(p^2+1,5)+\frac{12145}{4}. \end{aligned}$$

References

[1] S.R. Blackburn, P.M. Neumann, and G. Venkataraman, *Enumeration of finite groups*, Cambridge Tracts in Mathematics, 173, Cambridge University Press, 2007.

[2] W. Bosma, J. Cannon and C. Playoust, *The Magma algebra system I: The user language*, J. Symb. Comp. **24** (1997), 235–265.

[3] Marcus du Sautoy and Michael Vaughan-Lee, *Non-PORC behaviour of a class of descendant p-groups*, J. Algebra **361** (2012) 287–312.

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

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

[6] G. Higman, *Enumerating p-groups. I: Inequalities*, Proc. London Math. Soc. **(3) 10** (1960), 24–30.

[7] G. Higman, *Enumerating p-groups. II: Problems whose solution is PORC*, Proc. London Math. Soc. **(3) 10** (1960), 566–582.

[8] I.G. Macdonald, *Symmetric functions and Hall polynomials*, Second edition. Oxford Mathematical Monographs. The Clarendon Press, Oxford University Press, New York, 1995.

[9] 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.

[10] L. Pyber, *Enumerating finite groups of given order*, Ann. of Math. (2) **137** (1993), 203–220.

[11] Charles C. Sims, *Enumerating p-groups*, Proc. London Math. Soc. **(3) 15** (1965), 151–166.

[12] Brett Witty, *Enumeration of groups of prime-power order*, Phd thesis, Australian National University, 2006. (http://www.brettwitty.net/phd.php)