Graham Higman's PORC conjecture

Michael Vaughan-Lee

October 2011

Abstract

We survey the history of Graham Higman's PORC conjecture concerning the form of the function $f(p^n)$ enumerating the number of groups of order p^n. The conjecture is that for a fixed n there is a finite set of polynomials in p, $g_1(p)$, $g_2(p)$, ..., $g_k(p)$, and a positive integer N, such that for each prime p, $f(p^n) = g_i(p)$ for some i $(1 \leq i \leq k)$ with the choice of i depending on the residue class of p modulo N. We describe some properties of a group recently discovered by Marcus du Sautoy which has major implications for the PORC conjecture.

1 Introduction

Mathematicians love to count things. How many possibilities are there for a Sudoku solution grid? How many Latin squares of order 4 are there? How many groups are there of order 8? Answers: 6,670,903,752,021,072,936,960, 576 and 5. I found the answers to the first two questions in Wikipedia. The answer to the third question has been known to group theorists for well over 100 years. For a short modern analysis of the groups of order 8 see Section 4.4 of Hall [8]. Often the answers to this sort of question involve a classification of all the possibilities, and perhaps a complete list of the possibilities. As mentioned above, the five groups of order 8 have been well understood for well over 100 years, but it might be a bit tricky to produce a list of all the Sudoku solution grids. It would be perfectly possible (though tedious!) to draw up a complete list of the 576 Latin squares of order 4 by hand. However, a little thought enables you to see that there are 576 Latin squares of order 4 without actually listing them all. Let L be a Latin square of order n, and assume that the entries in the cells of the square are integers in the range $\{1, 2, \ldots, n\}$. We say that L is reduced if the entries in the first row and first column are in their natural order $1, 2, \ldots, n$. It is easy to see that the total number of Latin squares of order n is $n!(n-1)!$ times the number of reduced Latin squares of order n. And it is easy to see that there are exactly 4 reduced Latin squares of order 4:

$$\begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \\ 3 & 4 & 1 & 2 \\ 4 & 1 & 2 & 3 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \\ 3 & 1 & 4 & 2 \\ 4 & 3 & 2 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 2 & 1 \\ 4 & 3 & 1 & 2 \end{bmatrix}.$$

It immediately follows that there are 576 Latin squares in all. If we also allow ourselves to permute the names of the symbols then we are left with just two Latin squares of order 4:

$$\begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \\ 3 & 4 & 1 & 2 \\ 4 & 1 & 2 & 3 \end{bmatrix}.$$

These two Latin squares give the group multiplication tables for the two groups of order 4, the Klein four-group and the cyclic group of order 4.

$\times$	1	a	b	ab
1	1	a	b	ab
a	a	1	ab	b
b	b	ab	1	a
ab	ab	b	a	1

,

$\times$	1	a	a^2	a^3
1	1	a	a^2	a^3
a	a	a^2	a^3	1
a^2	a^2	a^3	1	a
a^3	a^3	1	a	a^2

.

The total number of Latin squares of order n is bounded by n^{n^2}. (There are n^2 cells, and n choices for the entry in each cell.) You can do a little better than this if you note that there are n rows, and $n!$ possibilities for the entries in any given row, so that the total number of Latin squares is bounded by $(n!)^n$. The best bounds do not seem to do a lot better than this. J.H. van Lint and R.M. Wilson [20] show that if $L(n)$ is the total number of Latin squares of order n then

$$\frac{(n!)^{2n}}{n^{n^2}} \leq L(n) \leq \prod_{k=1}^{n} (k!)^{\frac{n}{k}}.$$

There are much tighter bounds for the number $f(n)$ of groups of order n. Pyber [17] has shown that

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

where $\mu(n)$ denotes the highest power to which any prime divides n. Note that there is no lower bound on $f(n)$ in this theorem, because the value of $f(n)$ is heavily dependant on the factorization of n into a product of primes. In particular, if n is prime then $f(n) = 1$. One of the main components in the proof of this result is a bound on the number of groups of prime-power order p^n given by Higman [9], improved by Sims [19], and further improved in unpublished work by Mike Newman and Craig Seeley.

$$p^{\frac{2}{27}n^3 - 6n^2} \leq f(p^n) \leq p^{\frac{2}{27}n^3 + O(n^{5/2})}.$$

The book *Enumeration of finite groups* by Blackburn, Neumann and Venkatamaran [2] gives a good account of the history of this problem.

Graham Higman's PORC conjecture is a conjecture about the precise form of the function $f(p^n)$, and we will return to the problem of enumerating groups of order p^n later. Meanwhile, as what might seem like a diversion, we will consider the problem of enumerating the algebras of dimension n over a field F.

2 Enumerating algebras of dimension n

By an algebra over a field F we mean a vector space A over F together with a product: for each pair of elements $a, b \in A$ there is a uniquely defined product $ab \in A$. The product is required to be bilinear, so that if $a, b, c \in A$ and $\lambda, \mu \in F$ then

$$\begin{aligned}(\lambda a + \mu b)c &= \lambda(ac) + \mu(bc),\\ c(\lambda a + \mu b) &= \lambda(ca) + \mu(cb).\end{aligned}$$

We do not require the product to satisfy any other conditions such as commutativity or associativity. If A is an algebra over F, and if we pick a basis $\{a_i \mid i \in I\}$ for A as a vector space over F then for each pair of basis elements a_i, a_j we can express the product $a_i a_j$ as a linear combination

$$a_i a_j = \sum_{k \in I} \lambda_{ijk} a_k$$

for some scalars $\lambda_{ijk} \in F$. These scalars are called *structure constants* for the algebra A. These structure constants completely determine the product on A since if $a = \sum_{i \in I} \alpha_i a_i$ and $b = \sum_{j \in I} \beta_j a_j$ are any two elements of A then using bilinearity we see that

$$ab = \sum_{i,j,k \in I} \alpha_i \beta_j \lambda_{ijk} a_k.$$

Note however that if we pick a different vector space basis for A then we may get a different set of structure constants, so that different sets of structure constants can give the same algebra A. We will return to this point shortly.

If F is an infinite field then there are infinitely many choices for sets of structure constants. But there is a unique finite field $\mathbb{F}_q$ of order q for every prime-power q, and if A is an algebra of dimension n over $\mathbb{F}_q$ then there are exactly q^{n^3} possible sets of structure constants $\{\lambda_{ijk} \mid 1 \leq i, j, k \leq n\}$ for A. So there is an upper bound of q^{n^3} for the number $g(n, q)$ of n-dimensional algebras over $\mathbb{F}_q$. (But remember that different sets of structure constants can give the same algebra, so $g(n, q)$ is less than this upper bound.) This means that, for fixed n, $g(n, q)$ is bounded by a polynomial in q. Graham Higman [10] proved a much stronger result than this. He showed that, for fixed n, $g(n, q)$ is **P**olynomial **O**n **R**esidue **C**lasses — PORC. This means that there is a finite set of polynomials in q, $g_1(q)$, $g_2(q)$, ..., $g_k(q)$, and a positive integer N, such that for any prime-power q

$$g(n, q) = g_i(q)$$

for some i ($1 \leq i \leq k$), with the choice of i depending on the residue class of q modulo N. For example, if $n = 2$ then we have three polynomials. If q is a power of 2 then $g(2, q) = q^4 + q^3 + 4q^2 + 3q + 6$, if q is a power of 3 then $g(2, q) = q^4 + q^3 + 4q^2 + 4q + 6$, and if q is a power of p with $p > 3$ then $g(2, q) = q^4 + q^3 + 4q^2 + 4q + 7$. So we can take $N = 6$, and the choice of polynomial depends on the residue class of q modulo

6. When $n = 3$ there are 22 polynomials of degree 18, with the choice of polynomial depending on the residue class of q modulo $4 \times 3 \times 5 \times 7$.

Higman's proof of this result is far too long and difficult to give here, but we can illustrate many of the key ideas in Higman's proof by looking at how the polynomials above for $n = 2$ can be obtained.

First we investigate how a change of basis affects the structure constants. We might as well do this for general n. So let A be an algebra of dimension n over a field F and let $a_1, a_2, \ldots, a_n$ and $b_1, b_2, \ldots, b_n$ be two bases for A as a vector space over F. Let the sets of structure constants for these two bases be $\{\lambda_{ijk} \mid 1 \leq i, j, k \leq n\}$ and $\{\mu_{ijk} \mid 1 \leq i, j, k \leq n\}$. We can express the elements of the second basis as linear combinations of elements of the first basis, and vice versa:

$$\begin{aligned} b_i &= \sum_{j=1}^{n} \alpha_{ji} a_j \ (1 \leq i \leq n), \\ a_j &= \sum_{k=1}^{n} \beta_{kj} b_k \ (1 \leq j \leq n), \end{aligned}$$

where $[\alpha_{ji}]$ and $\left[\beta_{kj}\right]$ are $n \times n$ matrices over F which are inverse to each other. So

$$\begin{aligned} b_i b_j &= \sum_{r,s=1}^{n} \alpha_{ri} \alpha_{sj} a_r a_s \\ &= \sum_{r,s,t=1}^{n} \alpha_{ri} \alpha_{sj} \lambda_{rst} a_t \\ &= \sum_{r,s,t,k=1}^{n} \alpha_{ri} \alpha_{sj} \lambda_{rst} \beta_{kt} b_k. \end{aligned}$$

It follows that

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

It is time to simplify the notation a bit! Each set of structure constants consists of n^3 elements of F, and we can think of these sets of structure constants as elements in an n^3-dimensional vector space V over F. The set of all non-singular $n \times n$ matrices over F form a group $\mathrm{GL}(n, F)$, the general linear group of degree n over F. The formula above defines an *action* of $\mathrm{GL}(n, F)$ on V. If $v = \{\lambda_{ijk} \mid 1 \leq i, j, k \leq n\} \in V$ and $g = [\alpha_{ji}] \in \mathrm{GL}(n, F)$ then we set $vg = \{\mu_{ijk} \mid 1 \leq i, j, k \leq n\}$, where μ_{ijk} is given by the formula above. (The formula also involves the matrix $\left[\beta_{kj}\right]$, but this matrix is the inverse of $[\alpha_{ji}]$ and so depends only on g.) This action of $\mathrm{GL}(n, F)$ on V satisfies three key properties.

1. If $u, v \in V$, $\alpha, \beta \in F$, and $g \in \mathrm{GL}(n, F)$ then $(\alpha u + \beta v)g = \alpha(ug) + \beta(vg)$.

2. If $v \in V$ and if I is the identity matrix in $\mathrm{GL}(n, F)$ then $vI = v$.

3. If $v \in V$ and $g, h \in \mathrm{GL}(n, F)$ then $v(gh) = (vg)h$.

There is also a fourth property which is critical for Higman's argument. This property is that the action of $[\alpha_{ji}]$ on V is given by a matrix in $\mathrm{GL}(n^3, F)$ whose entries are rational functions in the entries α_{ji}.

The three properties given above are easy to check, but I think we have had enough matrix algebra for now! Two elements $u, v \in V$ (i.e. two sets of structure constants) define the same algebra if and only if $u = vg$ for some $g \in \mathrm{GL}(n, F)$. In the jargon of *groups acting on sets* we say that two elements $u, v \in V$ define the same algebra if and only if they lie in the same orbit under the action of $\mathrm{GL}(n, F)$ on V. It is easy to see that "being in the same orbit" is an equivalence relation on V, so that the orbits partition V. The number of algebras of dimension n over F is the number of orbits in V under the action of $\mathrm{GL}(n, F)$.

If we take F to be the field $\mathbb{F}_q$ of q elements, then the number of orbits is $g(n, q)$ and Higman proves that this number is PORC. Actually, Higman proves a much more general result than this, but we can illustrate many of the key ideas that appear in Higman's proof by showing how to compute $g(2, q)$.

So let $n = 2$, and consider the action of $\mathrm{GL}(2, \mathbb{F}_q)$ on V described above. Note that when $n = 2$ then V has dimension 8. The number of orbits of $\mathrm{GL}(2, \mathbb{F}_q)$ on V can be computed using a result which is often called Burnside's Lemma [3], though some people think this is a misnomer. If $g \in \mathrm{GL}(2, \mathbb{F}_q)$ then we define $\mathrm{fix}(g) = \{v \in V \mid vg = v\}$. The number of orbits is then given by the formula

$$\frac{1}{|\mathrm{GL}(2, \mathbb{F}_q)|} \left(\sum_{g \in \mathrm{GL}(2, \mathbb{F}_q)} |\mathrm{fix}(g)| \right).$$

It follows from properties (2) and (3) above that if g and h are conjugate elements of $\mathrm{GL}(2, \mathbb{F}_q)$ (i.e. if $h = x^{-1}gx$ for some $x \in \mathrm{GL}(2, \mathbb{F}_q)$) then $|\mathrm{fix}(g)| = |\mathrm{fix}(h)|$. Two elements in $\mathrm{GL}(n, F)$ are conjugate if and only if they have the same rational canonical form. However we do not have to concern ourselves with the rational canonical form in the case $n = 2$, since two elements in $\mathrm{GL}(2, \mathbb{F}_q)$ are conjugate if and only if they have the same minimum polynomial. The minimum polynomial of a matrix in $\mathrm{GL}(2, \mathbb{F}_q)$ will have degree one or two. The roots of the minimum polynomial of an element $g \in \mathrm{GL}(2, \mathbb{F}_q)$ are the eigenvalues of g. These may not lie in $\mathbb{F}_q$, but they will lie in some extension field of $\mathbb{F}_q$, so allowing roots in an extension field we have three types of minimum polynomial that can arise:

$$(x - \lambda),\ (x - \lambda)^2,\ (x - \lambda)(x - \mu)$$

with $\lambda, \mu \neq 0$, $\lambda \neq \mu$. The first case corresponds to $g = \begin{bmatrix} \lambda & 0 \\ 0 & \lambda \end{bmatrix}$. In the second case g has a repeated eigenvalue, but is not diagonalizable — in this case g is conjugate to $\begin{bmatrix} \lambda & 1 \\ 0 & \lambda \end{bmatrix}$. In the third case g has two distinct eigenvalues which may or may not lie in $\mathbb{F}_q$.

For each $g \in \mathrm{GL}(2, \mathbb{F}_q)$ we can compute the matrix $A(g)$ giving the action of g on V. Property (1) above implies that $\mathrm{fix}(g)$ is a subspace of V, and so $|\mathrm{fix}(g)| = q^k$ where k is the dimension of $\mathrm{fix}(g)$. This dimension k is the dimension of the eigenspace of $A(g)$ corresponding to eigenvalue 1.

If $g = \begin{bmatrix} \lambda & 0 \\ 0 & \lambda \end{bmatrix}$ then $A(g)$ equals

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

so $\mathrm{fix}(g)$ has dimension 0 unless $\lambda = 1$, in which case it has dimension 8.

If g in conjugate to $\begin{bmatrix} \lambda & 1 \\ 0 & \lambda \end{bmatrix}$ then $A(g)$ is conjugate to

$$\begin{bmatrix} \lambda & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \lambda & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \lambda & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \lambda & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \lambda & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \lambda & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \lambda & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & \lambda \end{bmatrix} \text{ or } \begin{bmatrix} \lambda & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \lambda & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \lambda & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \lambda & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \lambda & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \lambda & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \lambda & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & \lambda \end{bmatrix}$$

$$\text{or } \begin{bmatrix} \lambda & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \lambda & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \lambda & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \lambda & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \lambda & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \lambda & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \lambda & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & \lambda \end{bmatrix},$$

depending on whether q is a power of 2, a power of 3, or a power of p for a prime $p > 3$.

Finally if g has distinct eigenvalues λ, μ then $A(g)$ has eigenvalues

$$\lambda, \lambda, \lambda, \mu, \mu, \mu, \lambda^2\mu^{-1}, \lambda^{-1}\mu^2.$$

In this case, if $\lambda, \mu \in \mathbb{F}_q$ then $A(g)$ is conjugate to a diagonal matrix with these eigenvalues along the diagonal. If $\lambda, \mu \notin \mathbb{F}_q$ then $A(g)$ is not conjugate to a diagonal

matrix in $\mathrm{GL}(8,\mathbb{F}_q)$, but it is conjugate to a diagonal matrix in $\mathrm{GL}(8,K)$ for any extension field K of $\mathbb{F}_q$ containing λ and μ. In either case, the dimension of $\mathrm{fix}(g)$ is the number of 1's in the sequence $\lambda,\lambda,\lambda,\mu,\mu,\mu,\lambda^2\mu^{-1},\lambda^{-1}\mu^2$.

It is now easy to check the following.

- If g has minimum polynomial $x-1$ then $\mathrm{fix}(g)$ has dimension 8.
- If g has minimum polynomial $(x-1)^2$ then $\mathrm{fix}(g)$ has dimension 4 if q is a power of 2 and dimension 3 if q is not a power of 2.
- If g has minimum polynomial $(x-1)(x+1)$ then $\mathrm{fix}(g)$ has dimension 4. (Note that if q is a power of 2 then $(x-1)(x+1)=(x-1)^2$.)
- If g has minimum polynomial $(x-1)(x-\mu)$ with $\mu\neq 0,1,-1$ then $\mathrm{fix}(g)$ has dimension 3.
- If g has minimum polynomial $(x-\lambda)(x-\lambda^2)$ with $\lambda\neq 0,\pm 1$, $\lambda^3\neq 1$ then $\mathrm{fix}(g)$ has dimension 1.
- If g has minimum polynomial $(x-\lambda)(x-\lambda^2)$ with $\lambda\neq 1$, $\lambda^3=1$, then $\mathrm{fix}(g)$ has dimension 2. Note that this cannot arise if q is a power of 3.
- In all other cases $\mathrm{fix}(g)$ has dimension 0.

In each case $|\mathrm{fix}(g)|$ is PORC. Note that these 7 cases arise from subdividing the three types of minimal polynomial according to whether or not the eigenvalues satisfy various *monomial* equations, such as $\lambda=1$, $\lambda^2=1$, $\lambda^3=1$, $\lambda^2\mu^{-1}=1$. It is not really necessary here, but you can also distinguish between eigenvalues in $\mathbb{F}_q$ and eigenvalues not in $\mathbb{F}_q$ with monomial equations: λ is a root of an irreducible quadratic over $\mathbb{F}_q$ if $\lambda^{q-1}\neq 1$, $\lambda^{q^2-1}=1$; and μ is the other root of the same irreducible quadratic if $\lambda^q\mu^{-1}=1$.

To compute the number of orbits we also need to know how many g lie in each of the seven categories just listed. The numbers are as follows.

- There is 1 element g with minimum polynomial $x-1$ (the identity element).
- There are q^2-1 elements with minimum polynomial $(x-1)^2$.
- If q is odd there are q^2+q elements with minimum polynomial $(x-1)(x+1)$. If q is a power of 2 this case does not arise.
- If q is a power of 2 there are $(q-2)q(q+1)$ elements with minimum polynomial $(x-1)(x-\mu)$ with $\mu\neq 0,1,-1$; and if q is odd there are $(q-3)q(q+1)$ elements.
- If q is a power of 2 and $q\equiv 1 \bmod 3$ then there are $(q-4)q(q+1)$ elements with minimum polynomial $(x-\lambda)(x-\lambda^2)$ with $\lambda\neq 0,\pm 1$, $\lambda^3\neq 1$; if q is a power of 2 and $q\equiv 2 \bmod 3$ then there are $(q-2)q(q+1)$ elements; if q is a power of 3 then there are $(q-3)q(q+1)$ elements; if q is a power of p for $p>3$ and if $q\equiv 1 \bmod 3$ there are $(q-5)q(q+1)$ elements; and if q is a power of p for $p>3$ and $q\equiv 2 \bmod 3$ then there are $(q-3)q(q+1)$ elements.

- If $q = 3^k$ there are no elements with minimum polynomial $(x-\lambda)(x-\lambda^2)$ with $\lambda \neq 1$, $\lambda^3 = 1$; if $q \equiv 1 \bmod 3$ there are $q(q+1)$ elements; and if $q \equiv 2 \bmod 3$ there are $q(q-1)$ elements.

- The number of elements in this last category is $|\mathrm{GL}(2, \mathbb{F}_q)|$ minus the sum of all the numbers of elements in the other 6 categories.

All these numbers are PORC, and it follows that the number of orbits, $g(2,q)$, is PORC. The three polynomials giving the value of $g(2,q)$ depending on whether q is a power of 2, a power of 3, or a power of p for some $p > 3$ can be obtained by feeding these numbers into the formula for the number of orbits of $\mathrm{GL}(2, \mathbb{F}_q)$ on V.

3 Enumerating the groups of order p^n

As we saw in the Introduction, Higman [9] proved that for fixed n the number of groups of order p^n, $f(p^n)$, is bounded by a polynomial in p. Higman conjectured that (for fixed n) $f(p^n)$ is PORC — this is his famous PORC conjecture. The conjecture has been proved correct for $n \leq 7$. The table below gives the number of groups of order p^n for $n \leq 5$.

	$p=2$	$p=3$	$p \geq 5$
p	1	1	1
p^2	2	2	2
p^3	5	5	5
p^4	14	15	15
p^5	51	67	$2p + 61 + 2\gcd(p-1,3) + \gcd(p-1,4)$

There are 267 groups of order 2^6 and 504 groups of order 3^6. For $p \geq 5$ the number of groups of order p^6 is

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

The numbers of groups of order 2^7, 3^7, 5^7 are respectively 2328, 9310, 34297. For $p > 5$ the number of groups of order p^7 is

$$\begin{aligned} &3p^5 + 12p^4 + 44p^3 + 170p^2 + 707p + 2455 \\ &+(4p^2 + 44p + 291)\gcd(p-1,3) + (p^2 + 19p + 135)\gcd(p-1,4) \\ &+(3p + 31)\gcd(p-1,5) + 4\gcd(p-1,7) + 5\gcd(p-1,8) \\ &+\gcd(p-1,9). \end{aligned}$$

So, for example, for $p \geq 5$ the number of groups of order p^6 is one of 8 polynomials in p, where the choice of polynomial depends on the residue class of p modulo 60. The PORC conjecture is still open for $n = 8$.

The groups of order p^2 were classified by Netto [13] in 1882. The groups of order p^3 were independently determined by Cole and Glover [4], Hölder [11] and Young [21] in 1893. The groups of order p^4 were determined by Hölder [11] and Young [21]. The groups of order p^5 were classified by Bagnera [1] in 1898. However it was not until 2004 that Newman, O'Brien and Vaughan-Lee [14] classified the groups of order p^6. The groups of order p^7 were classified by O'Brien and Vaughan-Lee [16] in 2005.

Higman [10] proves that the number of groups of order p^n with p-class 2 is PORC (for any fixed n). The Frattini subgroup of a p-group G is the subgroup generated by the p-th powers $\{x^p \mid x \in G\}$ and the commutators $\{[x,y] \mid x,y \in G\}$ (where $[x,y]$ denotes $x^{-1}y^{-1}xy$). We say that G has p-class 2 if the Frattini subgroup is elementary abelian and central, that is to say if

$$[x^p, y] = 1,\ x^{p^2} = 1,\ [[x,y],z] = 1,\ [x,y]^p = 1$$

for all $x, y, z \in G$. (Higman uses the term Φ-class 2.) Evseev [7] has extended Higman's result to the more general class of p-groups in which the derived group is elementary abelian and central, that is groups satisfying

$$[[x,y],z] = 1,\ [x,y]^p = 1$$

for all $x, y, z \in G$.

4 Immediate descendants

Nowadays the classification of p-groups of small order makes use of the lower exponent-p-central series of a group. If G is any group then the lower exponent-p-central series of G,

$$G = G_1 \geq G_2 \geq \ldots \geq G_i \geq \ldots,$$

is defined by setting $G_1 = G$, $G_2 = G'G^p$, and in general setting $G_{i+1} = [G_i, G]G_i^p$. If G is a finite p-group then $G_{c+1} = \{1\}$ for some c, and we say that G has p-class c if $G_c \neq \{1\}$, $G_{c+1} = \{1\}$. If G is a finite p-group of p-class $c > 1$ then we say that G is an *immediate descendant* of G/G_c. Apart from the elementary abelian group of order p^n, every group of order p^n is an immediate descendant of a group of order p^k for some $k < n$. To list the groups of order p^n, first list the groups of order p^k for all $k < n$. Then for each group G of order p^k for $k < n$, find all the immediate descendants of G which have order p^n.

So (for example) the formula given above for the number of p-groups of order p^6 ($p \geq 5$) can be obtained as follows. It turns out that for $p > 3$ there are 42 groups of order at most p^5 which have immediate descendants of order p^6. Each of these 42 groups is given by a presentation involving the prime p symbolically — for example one of the 42 groups has presentation

$$\langle a, b \mid a^p = [b,a,a], b^p = 1, \text{class } 3\rangle. \tag{1}$$

For each of these 42 groups we compute the number of immediate descendants of order p^6, and the formula given above is obtained by adding together each of these

individual contributions. For example, group (1) above has $p + \gcd(p-1, 3) + 1$ descendants of order p^6. Finally, we have to add one to this total to account for the elementary abelian group of order p^6. Each of the individual contributions is PORC, and as a consequence the formula above is PORC.

Higman does not use the term *immediate descendant*, and does not explicitly mention the lower exponent-p-central series. But nevertheless his theorem can be expressed in these terms. Every group of order p^n and p-class 2 is an immediate descendant of the elementary abelian group of order p^r for some $r < n$. If G has order p^{r+s}, and if G is an immediate descendant of the elementary abelian group of order p^r then in Higman's terminology we say that G has Φ-complexion (r, s). Higman defines $g(r, s; p)$ to be the number of groups with Φ-complexion (r, s). So the number of p-class 2 groups of order p^n is

$$\sum_{r+s=n} g(r, s; p).$$

If we let V be a vector space of dimension r over $\mathbb{F}_p$, and if we let $V \wedge V$ be the exterior square of V, then $\mathrm{GL}(r, p)$ induces an action on the direct sum $V \oplus (V \wedge V)$, in much the same way as $\mathrm{GL}(n, p)$ induces an action on sets of structure constants for algebras of dimension n. Higman shows that if $p > 2$ then $g(r, s; p)$ is equal to the number of orbits under this action on subspaces of codimension s in $V \oplus (V \wedge V)$. Higman uses his theorem on the number of orbits in a vector space under the action of general linear groups to show that this number is PORC. In fact his theorem shows that the number of orbits of subspaces of dimension *at most* s is PORC, and he obtains the number of orbits of subspaces of dimension s as the difference between the number of orbits of susbspaces of dimension at most s and the number of orbits of subspaces of dimension at most $s - 1$.

Marcus du Sautoy has found a group G_p of order p^9 with the property that the number of immediate descendants of G_p of order p^{10} is *not* PORC. We will describe this group and some of its properties in Section 5 below. However Marcus's example does not disprove the PORC conjecture. As we have seen, the total number of groups of order p^{10} is obtained by adding together the number of immediate descendants of order p^{10} of each group of order less than p^{10}, and then adding 1 to the total to account for the elementary abelian group of order p^{10}. The grand total might still be PORC, even though we know that one of the individual summands is not PORC. My own view is that this is extremely unlikely. But in any case I believe that Marcus's group provides a counterexample to what I hazard to call the *philosophy* behind Higman's conjecture. Higman obtains the number of groups of order p^n of p-class 2 by adding up the number of immediate descendants of order p^n of all the elementary abelian groups of order less than p^n. He shows that the grand total is PORC by proving that all the individual summands are PORC. Each of the individual summands is the difference of two PORC functions obtained from his theorem on the action of general linear groups. And, as we saw in Section 2, this theorem is obtained by splitting the elements of the general linear group into a number of distinct classes with the property that the number of elements in each class is PORC, and with the property

that for each class C there is a single PORC function giving the value of $|\mathrm{fix}(g)|$ for $g \in C$.

5 Marcus du Sautoy's group

Marcus du Sautoy's group has the following presentation for all $p > 3$:

$$G_p = \left\langle \begin{array}{c} x_1, x_2, x_3, x_4, x_5, x_6, y_1, y_2, y_3 : [x_1, x_4] = y_3, [x_1, x_5] = y_1, [x_1, x_6] = y_2 \\ [x_2, x_4] = y_1, [x_2, x_5] = y_3, [x_3, x_4] = y_2, [x_3, x_6] = y_1 \end{array} \right\rangle$$

where all other commutators are defined to be 1, and where $g^p = 1$ for all $g \in G_p$.

The group is a class two nilpotent group of order p^9. The quotient group G_p/G_p' is elementary abelian of order p^6, and G_p' is elementary abelian of order p^3. It turns out that both the order of the automorphism group of G_p and the number of conjugacy classes of G_p are not PORC.

In [6], du Sautoy and Vaughan-Lee prove the following result:

Let D_p be the number of descendants of G_p of order p^{10} and exponent p. Let V_p be the number of points (x, y) in $\mathbb{F}_p^2$ that satisfy $x^4 + 6x^2 - 3 = 0$ and $y^2 = x^3 - x$. Then

1. If $p \equiv 5 \bmod 12$ then $D_p = (p+1)^2/4 + 3$.
2. If $p \equiv 7 \bmod 12$ then $D_p = (p+1)^2/2 + 2$.
3. If $p \equiv 11 \bmod 12$ then $D_p = (p+1)^2/6 + (p+1)/3 + 2$.
4. If $p \equiv 1 \bmod 12$ and $V_p = 0$ then $D_p = (p+1)^2/4 + 3$.
5. If $p \equiv 1 \bmod 12$ and $V_p \neq 0$ then $D_p = (p-1)^2/36 + (p-1)/3 + 4$.

They also show that there are infinitely many primes $p \equiv 1 \bmod 12$ for which $V_p > 0$, but that there is no sub-congruence of $p \equiv 1 \bmod 12$ for which $V_p > 0$ for all p in that sub-congruence class.

So the number of descendants of G_p of order p^{10} and exponent p is not PORC. It follows easily from this that the number of descendants of G_p of order p^{10} is not PORC.

5.1 The conjugacy classes of G_p

The centre of G_p is the derived group G_p', and most elements outside G_p' have breadth 3 (i.e. they lie in conjugacy classes of size p^3). However some elements outside G_p' have breath 2 (i.e. they lie in conjugacy classes of size p^2). First we determine the elements of breadth 2 in the subgroup $\langle x_1, x_2, x_3 \rangle$. This subgroup is elementary abelian of order p^3. If $0 < \alpha < p$ then the elements x_2^α, x_3^α have breadth 2, but if $0 < \alpha, \beta < p$ then $x_2^\alpha x_3^\beta$ has breadth 3. We need to determine the elements of breadth 2 in $\langle x_1, x_2, x_3 \rangle$

which lie outside the subgroup $\langle x_2, x_3\rangle$, and so we consider an element $x_1x_2^dx_3^e$. The subgroup $[x_1x_2^dx_3^e, G_p]$ is generated by

$$y_1^dy_2^ey_3,\ y_1y_3^d,\ y_1^ey_2$$

and so $x_1x_2^dx_3^e$ has breadth 2 if p divides

$$\det\begin{bmatrix} d & e & 1 \\ 1 & 0 & d \\ e & 1 & 0 \end{bmatrix} = de^2 - d^2 + 1.$$

Now if $p|(de^2 - d^2 + 1)$ then $p|((de)^2 - d^3 + d)$ and so elements of breadth 2 of the form $x_1x_2^dx_3^e$ correspond to points on the elliptic curve $y^2 = x^3 - x$ over $\mathbb{F}_p$. Let E be the number of points on this curve, including the point at infinity. Then there are $E-2$ elements of breadth 2 of the form $x_1x_2^dx_3^e$. It follows that there are $(p-1)\times E$ elements of breadth 2 in the subgroup $\langle x_1, x_2, x_3\rangle$. There is an automorphism θ of G_p given by

$$x_1\theta = x_4,\ x_2\theta = x_5,\ x_3\theta = x_6,\ x_4\theta = x_1,\ x_5\theta = x_2,\ x_6\theta = x_3,$$

and it follows that the elements of breadth 2 in the subgroup $\langle x_4, x_5, x_6\rangle$ are of the form x_5^α, x_6^α, $(x_4x_5^dx_6^e)^\alpha$ with $0 < \alpha < p$ and with $p|(de^2 - d^2 + 1)$. A general element $g \in G_p$ can be written in the form $g = abc$ with $a \in \langle x_1, x_2, x_3\rangle$, $b \in \langle x_4, x_5, x_6\rangle$ and $c \in G_p'$. If abc has breadth 2 then a and b must either be trivial, or have breadth 2, and it is straightforward to show that the elements in G_p of breadth 2 are the following

$$x_2^\alpha x_5^\beta c,\ x_3^\alpha x_6^\beta c,\ (x_1x_2^dx_3^e)^\alpha(x_4x_5^dx_6^e)^\beta c,$$

where $0 \le \alpha, \beta < p$ and α, β are not both zero, where $p|(de^2 - d^2 + 1)$, and where $c \in G_p'$. So the total number of elements of breadth 2 in G_p is $(p^2-1)p^3 \times E$. It follows that the number of conjugacy classes of G_p is

$$p^6 + p^3 - 1 + (p^3 - p^2 - p + 1) \times E.$$

This number is *not* PORC. It is shown in Section 18.4 of [12] that if $p \equiv 3 \bmod 4$ then $E = p + 1$, but if $p \equiv 1 \bmod 4$ then $E = p + 1 - 2a$ where $p = a^2 + b^2$ with $a + ib \equiv 1 \bmod (2 + 2i)$. Note that a is uniquely determined by p. The Gaussian integers are a unique factorization domain, and we can write $p = (a + ib)(a - ib)$ where this factorization is unique up to unit factors ± 1, $\pm i$. The choice of a and b so that $a + ib \equiv 1 \bmod (2 + 2i)$ means that we take a to odd and b even, and we choose the sign of a so that $a - b \equiv 1 \bmod 4$. So the value of a is a function of p. But a (and hence E) cannot be a PORC function of p. To see this note that if a was a polynomial in p then the fact that $|a| < \sqrt{p}$ would imply that a was constant. So a could only be a PORC function of p if a took only finitely many values as p varies. However Dirichlet's theorem on primes in arithmetic progression implies that approximately half the primes are equal to $1 \bmod 4$. Putting this more precisely, if $\pi(x)$ is the number of primes less than x, then asymptotically $\pi(x) \sim \frac{x}{\log x}$, and if

we set $\pi'(x)$ equal to the number of primes less than x which are equal to $1 \bmod 4$, then $\pi'(x) \sim \frac{x}{2 \log x}$. However for a fixed a there can only be at most $\sqrt{x}$ primes less than x which have the form $a^2 + b^2$. So if a only took K distinct values as p varies, then there could only be at most $K\sqrt{x}$ primes less than x which are equal to $1 \bmod 4$. Asymptotically, $K\sqrt{x}$ is much less than $\pi'(x)$. So E is not PORC, and hence the number of conjugacy classes of G_p is not PORC.

5.2 The automorphism group of G_p

Let H be the automorphism group of G_p. Then H has a normal subgroup N of order p^{18} consisting of automorphisms mapping x_i to $x_i g_i$ for $i = 1, 2, \ldots, 6$, with $g_1, g_2, \ldots, g_6$ arbitrary elements of G_p'. The quotient group H/N acts as a group of automorphisms of G_p/G_p'. The quotient group G_p/G_p' is isomorphic as a group to the additive group of a 6-dimensional vector space over $\mathbb{F}_p$, and we can identify H/N with a subgroup of the general linear group $\mathrm{GL}(6, \mathbb{F}_p)$. If we reorder the generators of G_p in the order $x_1, x_4, x_2, x_5, x_3, x_6$ then it is easy to see that for every $A \in \mathrm{GL}(2, \mathbb{F}_p)$, and for every $u \in \mathbb{F}_p$ satisfying $u^4 = 1$, there is an element of H/N with action on G_p/G_p' given by the matrix

$$\begin{bmatrix} uA & 0 & 0 \\ 0 & u^{-1}A & 0 \\ 0 & 0 & A \end{bmatrix}.$$

There are $\gcd(p-1, 4)$ choices for u here, and $|\mathrm{GL}(2, \mathbb{F}_p)|$ choices for A. So these automorphisms give a subgroup $K/N \leq H/N$ of order $|\mathrm{GL}(2, \mathbb{F}_p)| \cdot \gcd(p-1, 4)$. For most primes ($\frac{11}{16}$ of them!) $H = K$, so that H has order $|\mathrm{GL}(2, \mathbb{F}_p)| \cdot \gcd(p-1, 4) \cdot p^{18}$. But if we can find $x, y \in \mathbb{F}_p$ satisfying $x^4 + 6x^2 - 3 = 0$ and $y^2 = x^3 - x$, then there are some additional automorphisms. Specifically, if we order the generators of G_p in their original order $x_1, x_2, x_3, x_4, x_5, x_6$, and if $x, y \in \mathbb{F}_p$ satisfy $x^4 + 6x^2 - 3 = 0$ and $y^2 = x^3 - x$, then if we let $d = x$ and $e = y/x$ and take

$$A = \begin{bmatrix} \frac{u(d^2+1)e}{4} & \frac{u(d^3+9d)e}{4} & \frac{u(d^3+5d)}{2} \\ \frac{u^{-1}(d^3+5d)e}{4} & -\frac{u^{-1}(d^2+5)e}{4} & \frac{u^{-1}(d^2+1)}{2} \\ 1 & d & e \end{bmatrix}$$

for any u with $u^4 = 1$, then there are elements in H/N with action on G_p/G_p' given by the matrix

$$\begin{bmatrix} \alpha A & 0 \\ 0 & \beta A \end{bmatrix}$$

for all $\alpha, \beta \neq 0$ in $\mathbb{F}_p$. In the cases when there do exist $x, y \in \mathbb{F}_p$ satisfying $x^4 + 6x^2 - 3 = 0$ and $y^2 = x^3 - x$, then these additional automorphisms together with automorphisms in K generate the full automorphism group H. (All this is described in detail in [6].)

The roots of the polynomial $x^2 + 6x - 3$ are $-3 \pm 2\sqrt{3}$. Now if $p > 3$ then 3 is a quadratic residue modulo p if and only if $p \equiv \pm 1 \bmod 12$, so we need $p \equiv \pm 1 \bmod 12$ to have any hope of solutions to our two equations.

The case $p \equiv -1 \bmod 12$ is straightforward. We need to solve $x^2 = -3 \pm 2\sqrt{3}$. Now $(-3+2\sqrt{3})(-3-2\sqrt{3}) = -3$, which is *not* a quadratic residue modulo p, so one of the two equations $x^2 = -3 \pm 2\sqrt{3}$ has two solutions, and the other has none. So we obtain two solutions $\pm d \in \mathbb{F}_p$ to the equation $x^4 + 6x^2 - 3 = 0$. We then want to solve the equations $y^2 = \pm(d^3 - d)$, and since -1 is *not* a quadratic residue modulo p one of these two equations will have two solutions, and the other will have none. So if $p \equiv -1 \bmod 12$ there are exactly two solutions to the two equations.

The case $p \equiv 1 \bmod 12$ is much trickier. In this case -3 *is* a quadratic residue modulo p, so the equation $x^4 + 6x^2 - 3 = 0$ either has no solutions in $\mathbb{F}_p$, or it has four solutions. It turns out that it has four solutions for approximately half the primes $p \equiv 1 \bmod 12$. This is because the splitting field of $x^4 + 6x^2 - 3$ has degree 8 over $\mathbb{Q}$, so that, by Chebotarev's density theorem, the primes p for which the polynomial splits over $\mathbb{F}_p$ have density $\frac{1}{8}$. These primes are necessarily equal to $1 \bmod 12$, and the primes equal to $1 \bmod 12$ have density $\frac{1}{4}$ by Dirichlet's theorem on primes in arithmetic progression. In the case when $x^4 + 6x^2 - 3 = 0$ has four solutions $\pm d_1, \pm d_2$ in $\mathbb{F}_p$ we still need to solve the equations $y^2 = \pm(d_1^3 - d_1)$ and $y^2 = \pm(d_2^3 - d_2)$. Since $p \equiv 1 \bmod 4$, -1 is a quadratic residue $\bmod p$, and so the equations $y^2 = \pm(d_1^3 - d_1)$ either have 0 solutions or 4 solutions. Similarly the equations $y^2 = \pm(d_2^3 - d_2)$ either have 0 solutions or 4 solutions. In fact the four equations either have 0 solutions or 8 solutions. To see this observe that

$$(d_1^3 - d_1)(d_2^3 - d_2) = (d_1^2 - 1)(d_2^2 - 1)d_1 d_2 = (-4 + 2\sqrt{3})(-4 - 2\sqrt{3})\sqrt{-3} = 4\sqrt{-3}.$$

If we pick $u \in \mathbb{F}_p$ such that $u^2 = -1$ then

$$(\frac{1}{4}(1+u)(d_1^3 + 5d_1))^4 = -3,$$

so $4\sqrt{-3}$ is a square in $\mathbb{F}_p$, and either both the equations $y^2 = d_1^3 - d_1$, $y^2 = d_2^3 - d_2$ have solutions in $\mathbb{F}_p$, or neither does.

It turns out that there are 8 solutions (x, y) to the two equations $x^4 + 6x^2 - 3 = 0$ and $y^2 = x^3 - x$ over $\mathbb{F}_p$ for approximately half the primes for which $x^4 + 6x^2 - 3$ splits. It is straightforward to see that if d is a root of $x^4 + 6x^2 - 3$ then $d^3 - d$ is a root of $x^4 + 360x^2 - 48$. Furthermore, if $x^4 + 360x^2 - 48$ has a root then so does $x^4 + 6x^2 - 3$. It follows that the two equations $x^4 + 6x^2 - 3 = 0$ and $y^2 = x^3 - x$ have solutions over $\mathbb{F}_p$ if and only if $x^8 + 360x^4 - 48$ has a root in $\mathbb{F}_p$. The splitting field of $x^8 + 360x^4 - 48$ has degree 16 over $\mathbb{Q}$, and so by Chebotarev's density theorem the primes p for which the polynomial splits over $\mathbb{F}_p$ have density $\frac{1}{16}$. These primes are necessarily equal to $1 \bmod 12$. In particular there are infinitely many primes $p \equiv 1 \bmod 12$ for which the two equations have 8 solutions. However the primes $p \equiv 1 \bmod 12$ for which $x^4 + 6x^2 - 3$ (or equivalently $x^4 + 360x^2 - 48$) have a root are extremely irregular. It is proved in [6] that if $p \equiv 1 \bmod 12$, and if we write $p = a^2 - 12b^2$ with $a, b > 0$ then $x^4 + 6x^2 - 3$ has a root in $\mathbb{F}_p$ if and only if $a \equiv 1 \bmod 3$. This means that you cannot capture the primes $p \equiv 1 \bmod 12$ for which there are roots in a sub-congruence class of $p \equiv 1 \bmod 12$. If $c \equiv 1 \bmod 12$ and $(c, d) = 1$ then a theorem due to Rademacher [18] implies that there are infinitely many primes $p \equiv c \bmod 12d$ where $p = a^2 - 12b^2$ with

$a > 0$ and $a \equiv 1 \bmod 3$, and infinitely many primes $p \equiv c \bmod 12d$ where $p = a^2 - 12b^2$ with $a > 0$ and $a \equiv 2 \bmod 3$.

It is proved in [6] that the order of the automorphism group of G_p is as follows:

- If $p \equiv 1 \bmod 12$ and there are no solutions to the equations $x^4 + 6x^2 - 3 = 0$ and $y^2 = x^3 - x$ over $\mathbb{F}_p$ then there are $|\mathrm{GL}(2,p)| \cdot 4p^{18}$ automorphisms.
- If $p \equiv 1 \bmod 12$ and there are solutions to the equations then there are $|\mathrm{GL}(2,p)| \cdot 36p^{18}$ automorphisms.
- If $p \equiv 11 \bmod 12$ there are $|\mathrm{GL}(2,p)| \cdot 6p^{18}$ automorphisms.
- If $p \equiv 5 \bmod 12$ there are $|\mathrm{GL}(2,p)| \cdot 4p^{18}$ automorphisms.
- If $p \equiv 7 \bmod 12$ there are $|\mathrm{GL}(2,p)| \cdot 2p^{18}$ automorphisms.

Since there are infinitely many primes $p \equiv 1 \bmod 12$ for which the equations have solutions, and since we cannot capture these primes in a sub-congruence class of $p \equiv 1 \bmod 12$, it follows that the order of the automorphism group of G_p is not PORC.

6 The p-group generation algorithm

We described in Section 5 how the order of the automorphism group of G_p is not PORC, and this is the reason that the number of descendants of G_p of order p^{10} is not PORC. To see why this is so we need to describe O'Brien's p-group generation algorithm [15] for computing the immediate descendants of a p-group G.

So let G be a finite p-group of p-class c. The p-covering group P of G is defined to be the largest finite p-group with a normal subgroup M satisfying the following three properties:

- $P/M \cong G$,
- $M \leq P^p P'$,
- M is central in P and of exponent p.

The p-covering group P is unique, and is actually quite easy to compute. The normal subgroup M is called the p-multiplier of G, and is also unique. Since G has p-class c it follows that $P_{c+1} \leq M$. (Recall from Section 3 that P_{c+1} is the $(c+1)^{th}$ term of the lower exponent-p-central series of P.) Since M is central and of exponent p, $P_{c+2} = \{1\}$. (It can happen that $P_{c+1} = \{1\}$.) A proper subgroup $S < M$ is said to be allowable if S is a supplement in M for P_{c+1}, that is if $SP_{c+1} = M$. The immediate descendants of G are the quotient groups P/S where S is an allowable subgroup. Note that if $P_{c+1} = \{1\}$ then there are no allowable subgroups, and hence no immediate descendants. In this case we say that G is terminal.

The automorphism group of G acts on M, and two immediate descendants P/S and P/T are isomorphic if and only if the allowable subgroups S and T are in the same orbit under the action of the automorphism group of G. So the bigger the automorphism group the smaller the number of immediate descendants.

We can describe Higman's analysis of the p-groups of p-class 2 in these terms. The p-groups of p-class 2 are immediate descendants of elementary abelian groups. Let G be an elementary abelian group of order p^r, and identify G with a vector space V of dimension r over $\mathbb{F}_p$. The p-multiplier of G is $V \oplus (V \wedge V)$. The p-class of G is 1, and in this case if P is the p-covering group then $P_2 = M = V \oplus (V \wedge V)$. So in this case every proper subgroup of M is allowable, and these subgroups correspond to proper subspaces of $V \oplus (V \wedge V)$. The automorphism group of G is $\mathrm{GL}(r, \mathbb{F}_p)$, and the number of immediate descendants of G is the number of orbits of proper subspaces of $V \oplus (V \wedge V)$ under the action of $\mathrm{GL}(r, \mathbb{F}_p)$.

7 Further problems

As we have seen, Graham Higman's PORC conjecture has been confirmed for $n \leq 7$. Higman has shown that the number of p-class two groups of order p^n is PORC for all n. Evseev has extended Higman's proof to show that the number of groups of order p^n with derived groups which are elementary abelian and central is PORC for all n.

What are the possibilities for extending these positive results, and what are the possibilities for actually settling the question completely? It should be possible to classify the groups of order p^8, though I believe that this will be extraordinarily difficult. Classifying the groups of order p^9 or p^{10} seems to be way out of reach for the time being. One possible way of making progress would be to aim for a combination of Higman's methods and classification methods. The hardest part of classifying the groups of order p^6 and p^7 was classifying the p-class two groups of those orders. In contrast, classifying the groups of maximal class of order p^6 and p^7 was relatively easy. You could settle the PORC conjecture for $n = 8$ if you could classify just those groups of order p^8 with p-class greater than two. However classifying the p-class three groups of order p^6 and p^7 was nearly as hard as classifying the p-class two groups. Nevertheless I believe that we could make substantial progress with groups of order p^8 by first classifying the groups of maximal class, and then looking at groups of coclass two, and so on.

It might be possible to extend Higman's result about groups of p-class two to groups of class two (without any restriction on the orders of the elements). But I believe that Marcus's group shows that it would be impossible to directly extend Higman's methods to p-class three groups, or even to class three groups of exponent p. As stated above, I believe that there is no immediate prospect of classifying all the groups of order p^{10}, or even of classifying all class 3 groups of exponent p and order p^{10}. We know that Marcus's group has a non-PORC number of immediate descendants of order p^{10}, but it seems likely that there are other class two groups of order p^9 which also have a non-PORC number of immediate descendants of order p^{10}. It is possible that the grand total of all class three groups of order p^{10} is PORC

even though some of the individual contributions to the total are non-PORC. But I do not see how to settle this without classifying this class of groups. Nevertheless it would be useful to find some more examples of class two groups of order p^9 with a non-PORC number of immediate descendants of order p^{10}. Even better would be to find some class two groups of order p^8 with a non-PORC number of immediate descendants of order p^9.

It is perhaps fitting to end this note with a mention of another remarkable result of Marcus du Sautoy [5]. Marcus proves that for each n there are finitely many subvarieties E_i $(i \in T)$ of a variety Y defined over $\mathbb{Q}$ and for each subset $I \subset T$ a polynomial $H_I(x)$ such that for almost all primes p

$$f(p^n) = \sum_{I \subset T} c_{p,I} H_I(p),$$

where

$$c_{p,I} = \text{card}\{a \in \overline{Y}(\mathbb{F}_p) \,|\, a \in \overline{E}_i(\mathbb{F}_p) \text{ if and only if } i \in I\}.$$

Here $\overline{Y}$ means reduction of the variety modulo p, which is defined for almost all p. Marcus's group G_p embeds the elliptic curve $y^2 = x^3 - x$ in its structure and there seems every reason to suppose that much more complicated algebraic varieties can be embedded in the structure of finite p-groups in such a way as to impact on the number of conjugacy classes, the size of the automorphism group and the number of descendants.

References

[1] Bagnera, G. *La composizione dei gruppi finiti il cui grado è la quinta potenza di un numero primo*, Ann. Mat. Pura Appl. (3) **1** (1898), 137–228.

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

[3] Burnside, W. *Theory of groups of finite order*, 2nd ed. Cambridge, 1911.

[4] Cole, F.N. and Glover, J.W. *On groups whose orders are products of three prime factors*, Amer. J. Math. **15** (1893), 1–4.

[5] du Sautoy, M.P.F. *Zeta functions and counting finite p-groups*, Electron. Res. Announc. Amer. Math. Soc. **5** (1999), 112–122.

[6] du Sautoy, M.P.F. and Vaughan-Lee, M.R. *Non-PORC behaviour of a class of descendant p-groups*, Preprint (2011).

[7] Evseev, A. *Higman's PORC conjecture for a family of groups*, Bull. London Math. Soc. **40** (2008), 415–431.

[8] Hall, M. *The theory of groups*, Macmillan, New York, 1959.

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

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

[11] Hölder, O. *Die Gruppen der Ordnungen p^3, pq^2, pqr, p^4*, Math. Ann. **43** (1893), 301–412.

[12] Ireland, K. and Rosen, M. *A classical introduction to modern number theory*, Graduate texts in mathematics, 84, Springer-Verlag, 1993.

[13] Netto, E. *Substitutionentheorie und ihre Anwendungen auf die Algebra*, Teubner, Leipzig (1882).

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

[15] O'Brien, E.A. *The p-group generation algorithm*, J. Symbolic Comput. **9** (1990), 677–698.

[16] O'Brien, E.A. and Vaughan-Lee, M.R. *The groups with order p^7 for odd prime p*, J. Algebra **292** (2005), 243–358.

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

[18] Rademacher, H. *Über die Anzahl der Primzahlen eines reell-quadratischen Zahlkörpers, deren Konjugierte unterhalb gegebener Grenzen liegen*, Acta Arithmetica **1** (1935), 67–77.

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

[20] van Lint, J.H. and Wilson, R.M. *A couse in combinatorics*, Cambridge University Press, 2001.

[21] Young, J.W.A. *On the determination of groups whose order is a power of a prime*, Amer. J. Math. **15** (1893), 124–178.