Counting p-groups and Lie algebras using PORC polynomials

Bettina Eick and Michael Vaughan-Lee

November 21, 2018

The four files

findtype, sizeclass, numberoffixedspaces, numberofsolutions

define four Magma functions

findtype(g), sizeclass(t), AllFixedSpaceNums(q, t),
NumberOfSolutions(A, k)

which we define below.

Let V be a finite dimensional vector space over the field GF(q).

If $g \in \mathrm{GL}(V)$ then findtype(g) returns the type of g.
If $g \in \mathrm{GL}(V)$ has type t then sizeclass(t) returns the size of the conjugacy class of g.
If $g \in \mathrm{GL}(V)$ has type t then AllFixedSpaceNums(q, t) returns a sequence of length $1 + \dim V$ giving the numbers of orbits of g on k-dimensional subspaces of V for $k = 0, 1, \ldots, \dim V$.

Suppose we are choosing elements $x_1, x_2, \ldots, x_k$ (say) from the extension field GF(q^n) of GF(q) subject to a finite set of equations of the form

$$x_1^{n_1} x_2^{n_2} \ldots x_k^{n_k} = 1 \qquad (1)$$

where $n_1, n_2, \ldots, n_k$ are integer polynomials in the Frobenius automorphism $x \mapsto x^q$ of GF(q^n). We write the equations as the rows of a matrix A, representing equation (1) by the row $[n_1, n_2, \ldots, n_k]$. Then NumberOfSolutions(A, k) returns the PORC formula for the number of choices of $x_1, x_2, \ldots, x_k$ satisfying the given set of equations. The number of solutions takes the form $a.f(q)$ where

1. a is an integer plus a linear combination of characteristic functions $\chi_{(i,N)}$, where $\chi_{(i,N)}(q) = 1$ if $q = i \bmod N$, and $\chi_{(i,N)}(q) = 0$ otherwise. (See Section 4 of our paper.)

2. f is a product of cyclotomic polynomials in q.

The function actually returns a and f as two separate values.

Example1, Example2, Example3, Example4 give four examples of sets of equations which actually arose in the computation of $G_{7,k}(q)$.

In Example1 and Example2 we are considering matrices of type

$$((1,(1)),(3,(1)),(3,(1))).$$

These matrices have eigenvalues $a, b, b^q, b^{q^2}, c, c^q, c^{q^2}$ satisfying $a^{q-1} = 1$, $b^{q^3-1} = 1$, $c^{q^3-1} = 1$, $b^{q-1} \neq 1$, $c^{q-1} \neq 1$, $bc^{-1} \neq 1$, $bc^{-q} \neq 1$, $bc^{-q^2} \neq 1$. In Example1 we have 5 equations:

$$a^{q-1} = 1,\ b^{q^3-1} = 1,\ c^{q^3-1} = 1,\ b^{q^2-1}c^{q^2-1} = 1,\ b^{q^2-q}c^q = 1,$$

and the number of solutions is $(1 + 6\chi_{(2,7)})(q-1)^2$. Equations 4 and 5 arise as follows. Let V have dimension 7 over $\mathrm{GF}(q)$, and suppose that $g \in \mathrm{GL}(V)$ has type

$$((1,(1)),(3,(1)),(3,(1))).$$

and eigenvalues $a, b, b^q, b^{q^2}, c, c^q, c^{q^2}$ satisfying

$a^{q-1} = 1$, $b^{q^3-1} = 1$, $c^{q^3-1} = 1$, $b^{q-1} \neq 1$, $c^{q-1} \neq 1$, $bc^{-1} \neq 1$, $bc^{-q} \neq 1$, $bc^{-q^2} \neq 1$.

Let $\overline{g}$ give the action of g on $(V \wedge V) \oplus V$. Then $\overline{g}$ has 28 eigenvalues

$$a, b, b^q, b^{q^2}, c, c^q, c^{q^2}, ab, ab^q, \ldots, ac^{q^2}, b^{q+1}, \ldots, c^{q^2+q},$$

and the type of $\overline{g}$ depends on which of these 28 eigenvalues are equal and which are not equal. Equation 4 corresponds to the eigenvalue bc being equal to the eigenvalue $b^{q^2}c^{q^2}$ and equation 5 corresponds to the eigenvalue b^q being equal to the eigenvalue $b^{q^2}c^q$.

In Example2 we have 9 equations, and the number of solutions is $(1 + 2\chi_{(1,3)})(q-1)$.

In Example3 and Example4 we are considering matrices of type

$$((1,(1)),(1,(1,1)),(2,(1)),(2,(1))).$$

These have eigenvalues a, b, b, c, c^q, d, d^q satisfying $a^{q-1} = 1$, $b^{q-1} = 1$, $c^{q^2-1} = 1$, $d^{q^2-1} = 1$.

You can run these examples by entering

```
load Examplei;
```

at the Magma prompt.