BULL. AUSTRAL. MATH. SOC. 20D60
VOL. 76 (2007) [479–480]

Enumeration of groups of prime-power order

BRETT E. WITTY

Finite group theorists have been interested in counting groups of prime-power order, as a preliminary step to counting groups of any finite order and to assist in explicitly listing such groups. In 1960, G. Higman considered when the functions giving the number of groups of prime-power order p^n, for fixed n and varying p, is of a particular form, called *polynomial on residue classes* (PORC). The suggestion that such counting functions are PORC is known as Higman's PORC conjecture. In his 1960 paper [**4**] he proved that a certain class of groups of prime-power order, now called exponent-p class two groups, have counting functions that are PORC, but did not furnish explicit PORC functions.

The aim of the project outlined in this thesis is to reinterpret Higman's proof to create and implement an algorithm that finds explicit results in this known case. The primary obstacle to this approach is that the prime p is variable, and hence, the results are in the form of PORC functions. This is the advantage of this method — it gives explicit enumeration results for infinitely many primes from a single calculation.

Chapter 1 of the thesis discusses some of the history of enumerating groups of prime-power order, and recent developments towards attempting to prove Higman's PORC conjecture. One of the primary computational results in the pursuit of the latter problem is O'Brien's method [**1**] to calculate the number of exponent-p class two groups of order p^n for *fixed* p and n.

Chapter 2 outlines the basic approach of the algorithm developed in the thesis. This approach is based on the theory developed by Higman [**4**] and involves several reductions that separate into isolated computational problems. The primary reduction is to reformulate the enumeration of exponent-p class two groups into a enumeration problem in linear algebra over finite fields, as given by Higman [**3**]. This linear algebraic problem reduces to a form of the Cauchy–Frobenius theorem ([**5**, p. 24]) for our particular setup. The rest of the approach involves formulating appropriate computational machinery for this form of the Cauchy–Frobenius Theorem. The computational machinery involves the structural theory of matrices over finite fields, as developed by Green [**2**], Higman [**4**], and Steinberg [**6**].

Received 12th July, 2007
Thesis submitted to the Australian National University, September 2006. Degree approved, May 2007.
Supervisor: Dr Michael F. Newman

Chapters 3 to 5 of the thesis discuss the relevant theory and algorithms behind each of the reductions discussed in Chapter 2. If these algorithms are implemented naïvely, the resulting program is far too slow to be practical. Chapter 6 outlines a few main combinatorial optimizations implemented to make calculations more practical.

Chapter 7 discusses results obtained from the computational machinery, as well as methods to verify that the calculation is correct. This computational approach is primarily combinatorial, ending in an inclusion-exclusion-type calculation over a large number of sets. For inputs close to the current state-of-the-art in group enumeration, this inclusion-exclusion calculation is prohibitively expensive. The final result in the thesis is a proposed "hybrid method". If we consider all the calculations in the main machinery except for the inclusion-exclusion calculations, then this subset of results can be obtained in reasonable time. The information gleaned from these calculations can be used to find information regarding the final answer: namely the degree of the PORC function and some of the structure of its coefficients. O'Brien's algorithm can find results for specific primes p. Using these results, the degree of the PORC function and Lagrange's interpolation theorem, we can obtain the PORC function itself without the expensive inclusion-exclusion calculations.

References

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

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

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

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

[5] D.F. Holt, B. Eick and E.A. O'Brien, *Handbook of computational group theory*, Discrete Mathematics and its Applications (Chapman and Hall/CRC, Boca Raton, FL, 2005).

[6] R. Steinberg, 'A geometric approach to the representations of the full linear group over a Galois field', *Trans. Amer. Math. Soc.* **71** (1951), 274–282.

9 Boronia Dr
Annandale, QLD 4814
Australia
e-mail: shorokin@hotmail com