ELECTRONIC RESEARCH ANNOUNCEMENTS
OF THE AMERICAN MATHEMATICAL SOCIETY
Volume 7, Pages 1–4 (February 12, 2001)
S 1079-6762(01)00087-7

# THE GROUPS OF ORDER AT MOST 2000

HANS ULRICH BESCHE, BETTINA EICK, AND E. A. O'BRIEN

(Communicated by Efim Zelmanov)

ABSTRACT. We announce the construction up to isomorphism of the 49 910 529 484 groups of order at most 2000.

## 1. INTRODUCTION

The problem of explicitly constructing all of the groups of a given finite order has a long and somewhat chequered history; its study was initiated by Cayley in 1854 when he determined the groups of order at most 6. The aim is to determine a complete and irredundant list of the groups of a given order: a representative of each isomorphism type is present and no two groups in the list are isomorphic. It is usually comparatively easy to generate a complete list; the difficulty lies in the reduction to distinct isomorphism types.

In practice, the difficulty experienced in constructing the groups of a given order is determined by the number of groups of that order. Higman [7] and Sims [14] provide asymptotic estimates which show that the number of groups of order $p^m$, for a prime $p$, is $p^{2m^3/27+O(m^{8/3})}$. Further, the number of groups of order $n$ depends on the prime factorisation of $n$: if $e(n)$ is the largest exponent of a prime dividing $n$, then Pyber [13] shows that the number of groups of order $n$ is at most $n^{(2/27+o(1))e(n)^2}$.

Historically, the approaches to the group construction problem involved a large number of hand computations and case distinctions, and focused on specific properties of the groups. They were consequently *ad hoc* in nature, and many contained errors. As one indicator of progress, the groups of order at most 100 were determined by 1980. We cite here three modern, significant, and accurate contributions: Hall and Senior [6], Neubüser [11], and Laue [8].

Here we announce a significant step forward in providing a solution to the group construction problem in its original form. We have developed *practical* algorithms to construct or enumerate the groups of a given order. While these methods rely on group-theoretic properties, they are inherently general-purpose. Motivated by the millennium, we used our implementations of these algorithms to enumerate

Received by the editors May 31, 2000.
2000 *Mathematics Subject Classification.* Primary 20D10, 20D15; Secondary 20-04.
*Key words and phrases.* Enumeration, determination, small groups, algorithms.
This work was supported in part by the Marsden Fund of New Zealand via grant #9144/3368248. Eick and O'Brien acknowledge the financial support of the Alexander von Humboldt Foundation, Bonn.

the 49 487 365 422 groups of order $2^{10}$, and to determine explicitly the 423 164 062 remaining groups of order at most 2000.

For a survey of the group construction problem, including an extensive bibliography, an outline of the algorithms used, and details of the construction of the groups of order at most 2000, we refer the reader to [1].

## 2. The algorithms

Our construction and enumeration algorithms were employed to determine the groups of order at most 2000. Here, we provide only the briefest summary of each algorithm and references to the primary sources for each. Naturally, the techniques used depend on inherent group-theoretic structural properties, such as nilpotence and solubility.

1. The $p$-group generation algorithm of Newman [9] and O'Brien [12]: given as input a $p$-group $P$, this algorithm constructs a complete and irredundant list of certain central extensions (*immediate descendants*) of $P$.
2. The $p$-group enumeration methods of Eick and O'Brien [4]: given as input a $p$-group $P$, these algorithms *count* the number of nonisomorphic immediate descendants of $P$.
3. The coprime split extension algorithm of Besche and Eick [2, 3]: given as input positive integers $r$, $s$ where $\gcd(|r|, |s|) = 1$, this algorithm determines up to isomorphism all groups of order $r \cdot s$ with normal Hall $r$-subgroup.
4. The Frattini extension method of Besche and Eick [2, 3]: this algorithm first determines candidates $F$ for Frattini factors of the soluble groups of order $n$; for each $F$, it now constructs Frattini extensions $G$ of order $n$ (that is, $G$ has normal subgroup $N$, where $N \leq \Phi(G)$ and $G/N \cong F$), and solves the isomorphism problem for the resulting list.
5. Algorithms to construct insoluble groups [1, 2]: given a perfect group $N$ as input and a positive integer $n$, this algorithm constructs those finite groups $G$ of order $n$ having soluble residuum $M \cong N$ (that is, $M$ is the smallest normal subgroup of $G$ with $G/M$ soluble).

A central requirement is that these algorithms are practical. Implementations of the algorithms are publicly available in the computer algebra systems GAP [5] or Magma [10].

## 3. The results

In Table 1, we list the ten most challenging orders, and the number of groups of each order. We enumerated the groups of order $2^{10}$; all other groups were explicitly constructed.

While it is practically possible to construct explicitly the groups of order $2^{10}$, we did not do so; of course, subsets of these groups can be constructed on demand using our implementations. We observe that 48 803 495 722 of these groups have exponent-2 class precisely 2.

The resulting catalogue of groups is published in electronic form; in particular, it is distributed with GAP and Magma as the Small Groups library. We also provide, as one component of the library, an algorithm to identify a given group in the library; see [1] for details. The library data was generated electronically, without intermediate hand computations.

TABLE 1. The ten most difficult orders

| Order | Number |
|---|---|
| $2^{10}$ | 49 487 365 422 |
| $2^9 \cdot 3$ | 408 641 062 |
| $2^9$ | 10 494 213 |
| $2^8 \cdot 5$ | 1 116 461 |
| $2^8 \cdot 3$ | 1 090 235 |
| $2^8 \cdot 7$ | 1 083 553 |
| $2^7 \cdot 3 \cdot 5$ | 241 004 |
| $2^7 \cdot 3^2$ | 157 877 |
| $2^8$ | 56 092 |
| $2^6 \cdot 3^3$ | 47 937 |

## 4. Future directions

Our algorithms and their implementations are publicly available and can be used to extend existing determinations. However, we believe that the new challenge is to construct "generic" groups—for example, those whose orders factorise in a certain way. As contributions in this direction, the SMALL GROUPS library includes those groups whose orders have at most 3 prime divisors; Besche and Eick [3] present an algorithm to determine the groups of order $p^n \cdot q$ for fixed prime power $p^n$ and arbitrary prime $q \neq p$.

## References

[1] Hans Ulrich Besche, Bettina Eick, and E. A. O'Brien, "A millennium project: constructing small groups", Preprint.

[2] Hans Ulrich Besche and Bettina Eick, "Construction of finite groups", *J. Symbolic Comput.* **27** (1999), 387–404. MR **2000c**:20001

[3] Hans Ulrich Besche and Bettina Eick, "The groups of order $q^n \cdot p$", *Comm. Algebra* 2001.

[4] Bettina Eick and E. A. O'Brien, "Enumerating $p$-groups", *J. Austral. Math. Soc. Ser. A* **67** (1999), 191–205. MR **2000h**:20033

[5] The GAP Group, GAP—*Groups, Algorithms, and Programming, Version* 4.2, Lehrstuhl D für Mathematik, RWTH Aachen and School of Mathematical and Computational Sciences, University of St Andrews, 2000.

[6] Marshall Hall, Jr., and James K. Senior, *The Groups of order* $2^n$ $(n \leq 6)$, Macmillan, New York, 1964. MR **29**:5889

[7] Graham Higman, "Enumerating $p$-groups. I: Inequalities", *Proc. London Math. Soc.* (3) **10** (1960), 24–30. MR **22**:4779

[8] Reinhard Laue, *Zur Konstruktion und Klassifikation endlicher auflösbarer Gruppen*, Bayreuth. Math. Schr. no. 9 (1982). MR **84e**:20018

[9] M. F. Newman, "Determination of groups of prime-power order", *Group Theory*, Lecture Notes in Math. **573** (Canberra, 1975), pp. 73–84, Springer-Verlag, Berlin, Heidelberg, New York, 1977. MR **56**:12115

[10] Wieb Bosma, John Cannon, and Catherine Playoust, "The MAGMA Algebra System I: The User Language", *J. Symbolic Comput.* **24** (1997), 235–265. MR **98f**:68006

[11] Joachim Neubüser, "Die Untergruppenverbände der Gruppen der Ordnungen $\leq$ 100 mit Ausnahme der Ordnungen 64 und 96", Habilitationsschrift, Kiel, 1967.

[12] E. A. O'Brien, "The $p$-group generation algorithm", *J. Symbolic Comput.* **9** (1990), 677–698. MR **91j**:20050

[13] László Pyber, "Asymptotic results for permutation groups", Amer. Math. Soc. DIMACS Series, **11** (DIMACS, 1991), 1993, pp. 197–219. MR **94g**:20003

[14] Charles C. Sims, "Enumerating $p$-groups", *Proc. London Math. Soc.* (3) **15** (1965), 151–166. MR **30:**164

Lehrstuhl D für Mathematik, RWTH Aachen, Templergraben 64, 52062 Aachen, Germany

*E-mail address*: `hbesche@math.rwth-aachen.de`

Fachbereich Mathematik, Universität Kassel, Heinrich-Plett-Str. 40, 34132 Kassel, Germany

*E-mail address*: `eick@mathematik.uni-kassel.de`

Department of Mathematics, University of Auckland, Private Bag 92019, Auckland, New Zealand

*E-mail address*: `obrien@math.auckland.ac.nz`