Computational Group Theory and the Classification of Finite Groups

Bettina Eick

Institut für Analysis und Algebra, Technische Universität Braunschweig, Germany

Abstract. The talk surveys the classification of finite groups from its origin to the most recent computational methods. In particular, the talk shows how the theory of groups is used in this part of computational group theory to design effective algorithms.

1 Introduction

In 1854, Cayley [7] introduced the abstract definition of a group: a group is a set G equipped with an associative multiplication, there exists an identity element in G and each element in G has an inverse. Directly connected to this abstract definition is the notion of isomorphism: two groups G and H are isomorphic if there is a bijection $f : G \to H$ that is compatible with the multiplication. Cayley also considered the question of classifying the groups of a given order up to isomorphism; his paper [7] has a list of groups of order at most 6. This was the starting point of the classification of groups up to isomorphism.

Each finite group G has a composition series; that is, a subnormal series $G = G_1 \rhd G_2 \rhd \ldots \rhd G_m \rhd G_{m+1} = \{1\}$ with simple quotients G_i/G_{i+1}. It is well-known that the finite *simple* groups are classified; that is, the composition factors of all finite groups are known. However, a general classification of all finite groups of a given order n is a still wide open topic up to today.

2 Comments on the history

The topic of classifying finite groups has a long history; we refer to [4] for detailed references. Here we exhibit some cornerstones of this history. Cayley's initial paper had immediately raised interest and a number of publications followed. By the year **1900**, the groups of square-free order and those whose order factorises into at most 3 primes had been determined as well as those of some fixed orders, such as 24 and 48. Around the year **1970**, the groups of order at most 200 except $2^7 = 128$ and $2^6 3 = 192$ had been obtained. All of these orders had been done by hand calculations yielding a total of 2 194 groups. The largest number of groups in this range are the 267 groups of order 2^6. From **1980** onwards, the classification of finite groups became a computational topic. The groups of order 128 were determined by O'Brien and the groups of order 192 by Besche and Eick. These two orders were the first that were only solved by computer. Note that there are 2 328 groups of order 128 and 1 543 groups of order 192. By the year **2000**, Besche, Eick and O'Brien had completed the classification of groups of order at most 2 000 except $1024 = 2^{10}$. There are a total of 423 164 062 groups of these orders. Among them, there are 10 494 213 groups of order 2^9 and 408 641 062 groups of order $2^9 \cdot 3$. The remaining orders sum up to 4 028 787 groups.

3 Aims and variations

We consider the following three variations of the aims in the group classification project.

(a) **Group construction.**
Determine a complete and irredundant list of groups of order n, so that each group of order n is isomorphic to exactly one group in the list.

(b) **Group construction and identification.**
Determine a complete and irredundant list of groups of order n, and an algorithm to identify a group of order n in the list.

(c) **Group enumeration.**
Determine the number $f(n)$ of groups of order n.

The aim (b) is the strongest and most desirable outcome. It also allows a significant cross-check of the determined group list; irredundancy follows directly from the group identification rountine and completeness can be supported by constructing groups with different approaches and comparing it to determined list with the group identification routine. The aim (c) is a significantly weaker aim than (a) or (b). It is often also difficult verify the result of a group enumeration independently. In summary, (a) and (b) are the preferred aims.

4 Construction algorithms

Let $n \in \mathbb{N}$ with prime-power factorisation $n = p_1^{e_1} \cdots p_m^{e_m}$. As a first step towards a construction of groups of order n, we use a case distinction:

(a) **Nilpotent groups.**
Each nilpotent group of order n is a direct product of its Sylow subgroups. Hence these groups can be constructed by determining the groups of orders $p_i^{e_i}$ and taking direct products.
(b) **Solvable, non-nilpotent groups.**
If n is not a prime, then each solvable group of order n has a non-trivial normal elementary abelian subgroup. This feature can be used to facilitate an induction approach.
(c) **Non-solvable groups.**
Each non-solvable group of order n has a composition factor that is non-abelian simple. Using the non-abelian simple groups as starting point, allows to construct these groups.

We discuss the used methods in more detail. First, the construction of finite p-groups of order p^e is facilitated by O'Brien's p-group generation algorithm [22]. This iterates over all groups G of order p^f for $f < e$ and determines the *descendants* of G. An implementation of this algorithm is available in the GAP package ANUPQ [12] and in Magma [6].

The GrpConst package [3] of GAP [13] offers two methods to construct solvable non-nilpotent groups: the Frattini extension method and the cyclic split extension method. The Frattini extension method is a general method to construct all solvable non-nilpotent groups of order n. Given such a group G, its Frattini subgroup $\Phi(G)$ is a nilpotent normal subgroup G such that $H = G/\Phi(G)$ has order dividing n and divisble by $p_1 \cdots p_m$. The structure of H has been investigated by Gaschütz [16]. As a result, it is known that $H = Soc(H) \rtimes K$, where $Soc(H)$ is a direct product of elementary abelian groups and K embeds into $Aut(Soc(H))$. This information allows to construct all possible candidates for the Frattini factors of the solvable non-nilpotent groups of order n directly up to isomorphism. Using these, the desired groups G of order n are now constructed as Frattini extensions of the Frattini factors H. This produces a complete list of groups of order n, that still needs to be reduced to isomorphism types. The random isomorphism test can be used to reduce the isomorphism problem effectively. We refer to Besche and Eick [3] for details.

There is a variety of methods to construct non-solvable groups known. The GrpConst package provides an algorithm that starts with the classification of perfect groups, see Holt and Plesken [19], and determines the desired groups from there. An alternative algorithm is described by Archer [1]. Among the groups of order at most 2000, there are only 1024 non-solvable groups; since this is a comparatively small number, their construction is a comparatively easy part of the group construction project.

The Handbook of Computational Group Theory by Holt, Eick and O'Brien [18] gives background on computational methods in group theory in general and many details on this topic.

5 Results

The resulting group classifications are available in the SmallGroups Library. At current, this contains the groups of orders

- at most 2000 except 1024;
- square-free orders;
- cube-free orders at most 50 000; (see Dietrich and Eick [8])
- orders that factorise into at most 4 primes; (see Dietrich, Eick and Pan [9] and Pan [20])
- p^n for all primes p and $n \leq 7$; (see Girnat [14], Newman, O'Brien and Vaughan-Lee [17], and O'Brien and Vauhan-Lee [23])

The groups in the library are heavily cross-check, the data is identically available in GAP and Magma. A group identification method is included for many of the orders.

6 Current work

The work on the SmallGroups Library is ongoing up to today. Recently, Eick, Horn and Hulpke [10] used the available algorithms to extend the classification up to order 20 000 with few exceptions. Eick and Schanze [11] have added a group identification method for the groups of order 2^9, see also [21].

References

1. Claude Archer. *The extension problem and classification of nonsolvable groups.* PhD thesis, Université Libre de Bruxelles (1998).
2. Hans Ulrich Besche and Bettina Eick. *Construction of Finite Groups.* J. Symbolic Comput., **27**, 387–404, (1999).
3. Hans Ulrich Besche and Bettina Eick. *GrpConst: Construction of finite groups.* GAP Package, Available in GAP (2000).
4. H. U. Besche, B. Eick, and E. A. O'Brien. *A millennium project: constructing small groups.* Int. J. Algebra Comput., **12**, 623–644, (2002).
5. H. U. Besche, B. Eick, and E. O. Brien. *The SmallGroups Library.* Available in GAP and MAGMA) (2000).
6. Wieb Bosma, John Cannon and Catherine Playoust. em The MAGMA Algebra System I: The User Language. J. Symbolic Comput., **24**, 235–265 (1997).
7. Arthur Cayley. *On the Theory of Groups, as depending on the Symbolic Equation* $\theta^n = 1$. Philos. Mag. (4), **7**, 40–47 (1854).
8. H. Dietrich and B. Eick. *Groups of cube-free order.* J. Algebra **292**, 122 – 137 (2005).
9. H. Dietrich, B. Eick, and X. Pan. *Groups whose orders factorise into at most four primes.* J. Symbolic Comput. **108**, 23 – 40 (2022).
10. B. Eick, M. Horn, and A. Hulpke. *Constructing groups of 'small' order: recent results and open problems.* In Algorithmic and experimental methods in algebra, geometry, and number theory (Springer), 199 – 211 (2017).
11. Bettina Eick and Henrik Schanze. *The group identification problem for p-groups of small order.* arXiv:2603.09363 (2026).
12. G. Gamble, W. Nickel, and E. O'Brien. *ANUPQ: The ANU p-Quotient algorithm.* GAP package, Available in GAP (2025).
13. The GAP Group. *GAP – Groups, Algorithms, and Programming* see www.gap-system.org (2025).
14. B. Girnat. *Die Klassifikation der Gruppen bis zur Ordnung* p^5. arXiv:1806.07462 (2005).
15. Bettina Eick and E.A. O'Brien. *Enumerating p-groups.* J. Austral. Math. Soc. Ser. A, **67**, 191–205 (1999).
16. Wolfgang Gaschütz. *Über die Φ-Untergruppe endlicher Gruppen.* Math. Z., **58**, 160–170 (1953).
17. 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**, 383 – 401 (2003).
18. D. F. Holt, B. Eick and E. A. O'Brien, *Handbook of Computational Group Theory.* Discrete Mathematics and its Applications, Chapman & Hall/CRC (2005).
19. Derek F. Holt and W. Plesken. *Perfect Groups.* Clarendon Press, Oxford (1989).
20. Xueyu (Eileen) Pan. *SotGrps – Database of groups whose order factorises into at most 4 primes.* GAP package (2023).
21. H. Schanze. *IdPGroup: group identification for groups of order* 2^9. GAP package (2026). Available at `https://www.iaa.tu-bs.de/henschan/so.html`.
22. E.A. O'Brien. *The p-group generation algorithm.* J. Symbolic Comput. **9**, 677–698 (1990).
23. E. A. O'Brien and M. R. Vaughan-Lee. *The groups with order* p^7 *for odd prime p.* J. Algebra **292**, 243 – 258 (2005).