Constructing groups of 'small' order: Recent results and open problems

Bettina Eick, Max Horn and Alexander Hulpke

Abstract We investigate the state of the art in the computational determination and enumeration of the groups of small order. This includes a survey of the available algorithms and a discussion of their recent improvements. We then show how these algorithms can be used to determine or enumerate the groups of order at most 20 000 with few exceptions and we discuss the orders in this range which remain as challenging open problems.

1 Introduction

The determination of the groups of a given order n up to isomorphism is one of the central problems in finite group theory. The aim is to determine a list $\mathscr{L}_n$ of groups of order n so that every group of order n is isomorphic to exactly one group in the list $\mathscr{L}_n$. A slightly weaker but also interesting goal is to enumerate the isomorphism types of groups of a given order. The aim is to determine the cardinality $|\mathscr{L}_n|$, possibly without explicitly listing all groups in $\mathscr{L}_n$. There are asymptotic estimates known for $|\mathscr{L}_n|$, see Pyber [23] for a survey, but no closed formula for $|\mathscr{L}_n|$ is known. See also [11] for a discussion of properties of $|\mathscr{L}_n|$ as a function in n.

The history of this group construction or enumeration problem goes back to the beginnings of abstract group theory: Cayley [10] introduced the abstract definition

Bettina Eick
TU Braunschweig, Pockelsstraße 14, 38106 Braunschweig, Germany, e-mail: beick@tu-bs.de

Max Horn
Justus-Liebig-Universität Gießen, Arndtstraße 2, 35392 Gießen, Germany, e-mail: max.horn@math.uni-giessen.de

Alexander Hulpke
Colorado State University, Fort Collins, CO 80523-1874, USA, e-mail: hulpke@colostate.edu

of groups and determined the groups of order at most 6. Many other group constructions and enumerations followed the work of Cayley. We refer to Besche, Eick & O'Brien [7] for a history of group constructions and to Blackburn, Neumann & Venkataraman [8] for details on enumerations of groups.

Senior & Lunn [25, 26] determined all groups of order at most 200 except 128 and 192. It is quite remarkable that they did this by hand and got it right! A natural question is: why did they omit 128 and 192? Nowadays it is known that these two orders yield by far the most groups in the range of orders at most 200: using the SmallGroups library [5] one observes that there are 2 328 groups of order 128 and 1 543 of order 192, while the maximum is 267 for every other order at most 200. There are 6 065 groups of order at most 200 in total.

Why are there many groups for some orders and very few for others? For example, the SmallGroups library [5] asserts that there are 49 487 365 422 groups of order 1 024 and only 4 groups of order 1 025. The asymptotic results on $|\mathscr{L}_n|$ as reported in [23] as well as the known values for $|\mathscr{L}_n|$ in the SmallGroups library suggest that the largest multiplicity of a prime dividing an order n plays a major role; that is, if $n = p_1^{e_1} \cdots p_r^{e_r}$ for different primes $p_1, \ldots, p_r$, then $e = \max\{e_1, \ldots, e_r\}$ has a major impact on the number of groups of order n. Note that $1\,024 = 2^{10}$, while $1\,025 = 5^2 \cdot 41$.

Besche, Eick & O'Brien [6, 7] determined the groups of order at most 2 000 except 1 024 and Eick & O'Brien [15] enumerated the groups of order 1 024. The results are available in the SmallGroups library [5]. This group determination and enumeration was obtained with the massive help of computers and methods from computational group theory. The use of computers is essential due to the large numbers of groups. For example, there are eight orders in the range of orders at most 2 000 with more than 100 000 groups.

Since then, computer technology and also the methods from computational group theory have improved significantly. For example, a new isomorphism test and automorphism group algorithm has been developed by Cannon & Holt [9] and a new method to construct finite solvable groups has been introduced by Eick & Horn [12]. Further, many of the methods in the computer algebra system GAP [29] have been improved; in particular, the machinery to construct subdirect products has been significantly updated by the third author. The combination of these advances permits us to extend significantly the range of orders n for which $\mathscr{L}_n$ or at least $|\mathscr{L}_n|$ is computable.

It is the aim of this paper to report on the available group construction and enumeration methods in GAP [29] and its packages and their application to the determination or enumeration of groups of order at most 20 000. There are currently 39 orders in the range at most 20 000 for which the number of groups of these orders are unknown. We list these orders and discuss the difficulty that they impose on the group construction and enumeration methods. Thus we highlight the most challenging problems in the enumeration of finite groups of small orders.

The known numbers of groups $|\mathscr{L}_n|$ for $1 \leq n \leq 20\,000$ can be obtained at a webpage prepared by the second author:

`http://groups.quendi.de`.

Among these orders with known numbers, there are 56 orders with more than one million groups. For example, each of the orders of the form $2^9 \cdot p$ with p a prime yields more than 400 million groups. And the order 2^{10} yields more than one billion groups.

Acknowlegdement. We thank Eamonn O'Brien for comments on drafts of this work. The second author was supported by the DFG Schwerpunkt SPP 1489. The third author was supported by Simons Foundation Collaboration Grant 244502.

2 Algorithms to construct finite groups

In this section we give a brief overview of the available methods to construct finite groups. These methods fall into three different categories: methods to construct nilpotent groups, methods to construct solvable (non-nilpotent) groups and methods to construct non-solvable groups.

2.1 Construction of nilpotent groups

A finite nilpotent group is a direct product of its Sylow subgroups. Hence the construction of nilpotent groups directly translates to the construction of p-groups. For this purpose there is a well-established method available: the p-group generation method of O'Brien [21]. The basic approach of this method is to use induction along the lower exponent-p central series. An implementation of this method is available in the GAP package [19].

2.2 Construction of solvable (non-nilpotent) groups

The Frattini extension method.

The Frattini extension method by Besche & Eick [2] is a widely used method for the construction of finite solvable groups. Recall that the Frattini subgroup $\Phi(G)$ of a finite group G is the intersection of all maximal subgroups of G. The basic approach of this method is to determine up to isomorphism a list of candidates

for the Frattini factors of the groups of order n and then, for each candidate F, determine up to isomorphism all groups G of order n with $G/\Phi(G) \cong F$. The first step of this approach is usually comparatively fast and yields a comparatively short list of groups. It relies heavily on an effective determination of subdirect products. The second step is often more involved and requires the reduction of a given list of groups to isomorphism type representatives. A first reduction can often be achieved by using the highly effective random isomorphism test of [2]. A final reduction is then obtained by general isomorphism testing methods such as those described in [9, 27]. The Frattini extension method allows us readily to restrict to the construction of non-nilpotent groups or those with certain normal or non-normal Sylow subgroups. An implementation of this method is available in the GAP package [3].

Solvable group construction.

Eick & Horn [12] present an alternative method to construct the solvable groups of a given order. This is a direct generalisation of the p-group generation method. It is often slower than the Frattini extension method, but in some cases it was able to determine the groups of a given order where the Frattini extension method failed. Further, it is very useful in verifying the results of the Frattini extension method. Also this method restricts readily to construct non-nilpotent groups only. An implementation of this method in GAP exists and will be made available as a GAP package [17].

2.3 Construction of non-solvable groups

The cyclic extensions method.

Besche & Eick [2] outlined a rather crude approach towards constructing non-solvable groups. It starts from the library of perfect groups [16]; we refer to the work by Holt & Plesken [16] for this. It then iteratively constructs cyclic extensions of groups. The extensions obtained then must be reduced to isomorphism types. This requires an effective isomorphism test for non-solvable groups. Nowadays we use the method by Cannon & Holt [9] for this purpose whose implementation in GAP will be made available as part of GAP 4.9.

Archer's methods: supplements and $Z\phi$.

Archer [1] described two effective methods to construct the non-solvable groups of a given order n. Both approaches require that the perfect groups of all orders m dividing n are determined up to isomorphism; see [16].

The supplement method additionally requires that the solvable groups of order n/m are classified. For a given perfect group H of order m and a given solvable group

G of order n/m, it determines up to isomorphism all groups E having a normal subgroup $M \trianglelefteq E$ with $M \cong H$ and $E/M \cong G$.

The $Z\phi$ method additionally requires that all solvable groups of the orders kn/m are known, where k ranges over the sizes of the centers of the perfect groups of order m. For a given perfect group H of order m with center $Z = Z(H)$ of order k, it considers all solvable groups G of order kn/m extending Z and it determines up to isomorphism all groups E having a normal subgroup $M \trianglelefteq E$ with $M \cong H$ and $E/M \cong G/Z$. Note that the $Z\phi$ method does not apply in all cases on H; we refer to [1, Page 75] for details. Note also that [1, Section 5.1] contains a limited version of the $Z\phi$ method. This applies only if $|Z(H)| \leq 2$ and, if $|Z(H)| = 2$, then if $gcd(|Out(H)|, |G|) \leq 2$. While this is a significant restriction, it still applies to many of the cases that we need to consider.

Archer neither published the results of his enumeration, nor his implementations of the algorithms. We have implemented in GAP the limited version of the $Z\phi$ method. This does not apply to all cases, but it allows readily to be combined with the cyclic extension method. We are using this combination as an alternative approach to construct non-solvable groups. If the limited $Z\phi$ method applies, then it is usually more effective than the cyclic extension method. Our implementation of the limited $Z\phi$ method will be made available as a package for GAP.

As part of the applications of our implementation, we recomputed and extended the table on page 64 in [1]. We noted that the rows for $|S| \in \{128, 256\}$ in this table were incorrect. The correct values, as well as the additional value for $|S| = 384$, are as follows:

$\lvert S\rvert$	grps	$\mathscr{O}_K$	$\mathscr{O}_Z$	$\mathscr{O}_{Z,K}$
128	2 328	16 996	8 308	72 010
256	56 092	1 027 380	337 956	6 856 498
384	20 169	206 463	82 035	938 587

3 A symbolic enumeration algorithm

Suppose that $m \in \mathbb{N}$ is given and that the groups of order m are available; that is, $\mathscr{L}_m$ is known. In this section we describe an effective algorithm to enumerate the groups of order $m \cdot p$ for *all* primes p coprime to m. Our approach is based on a theorem by Taunt [28] and it extends the cyclic split extension method described in [2] and the ideas in [4].

For a group G of order m and $l \mid m$ let $\mathscr{O}_l$ denote a set of representatives of the $\mathrm{Aut}(G)$-classes of normal subgroups K in G with G/K cyclic of order l. For $K \in \mathscr{O}_l$ let $\mathrm{Aut}_K(G)$ denote the stabilizer of K in $\mathrm{Aut}(G)$, let $\overline{\mathrm{Aut}}_K(G)$ be the subgroup

of $\mathrm{Aut}(G/K)$ induced by the natural action of $\mathrm{Aut}_K(G)$ on G/K and let $\mathrm{ind}_K := [\mathrm{Aut}(G/K) : \overline{\mathrm{Aut}}_K(G)]$.

Let $(d_1,\ldots,d_k)$ be the list of all divisors of m, with $d_1 = 1$. We set

$$w(G) := (w_{d_1}(G),\ldots,w_{d_k}(G)), \quad \text{where} \quad w_{d_i}(G) := \sum_{K\in\mathscr{O}_{d_i}} \mathrm{ind}_K$$

and we denote

$$w(m) := (w_{d_1}(m),\ldots,w_{d_k}(m)), \quad \text{where} \quad w_{d_i}(m) := \sum_{G\in\mathscr{L}_m} w_{d_i}(G).$$

Theorem 1. *Let $m \in \mathbb{N}$ and π the set of those prime divisors of $(d_2-1)\cdots(d_k-1)$ that do not divide m.*

a) *Let p be a prime with $p \nmid m$. If there exists a group of order mp without normal Sylow p-subgroup, then $p \in \pi$.*

b) *Let p be a prime with $p \nmid m$. The number of isomorphism types of groups of order $m \cdot p$ having a normal Sylow p-subgroup is*

$$\sum_{\substack{i\in\{1,\ldots,k\}\\ \text{with } d_i \mid (p-1)}} w_{d_i}(m).$$

Proof. a) By Sylow's theorems the number of Sylow p-subgroups in a group of order mp is congruent to 1 modulo p and it divides m. Thus if there exists a group of order mp without normal Sylow p-subgroup, then $p \mid (d_i - 1)$ for some $i \in \{2,\ldots,k\}$. b) Suppose that H is group of order mp with normal Sylow p-subgroup. By the Schur-Zassenhaus theorem, $H \cong C_p \rtimes_\varphi G$ for a group G of order m and some homomorphism $\varphi : G \to \mathrm{Aut}(C_p) \cong C_{p-1}$. Taunt [28] proved that two split extensions $C_p \rtimes_{\varphi_1} G$ and $C_p \rtimes_{\varphi_2} G$ are isomorphic if and only if there exist $\alpha \in \mathrm{Aut}(G)$ and $\beta \in \mathrm{Aut}(C_p)$ so that $\varphi_1(\alpha(g)) = \beta^{-1}\varphi_2(g)\beta$ in $\mathrm{Aut}(C_p)$ for each $g \in G$. As $\mathrm{Aut}(C_p)$ is abelian, this reduces to $\varphi_1(\alpha(g)) = \varphi_2(g)$ for all $g \in G$ and thus is independent of β. Based on this, one can readily observe that the different isomorphism types of split extensions $C_p \rtimes_\varphi G$ with $K = \ker(\varphi)$ correspond one-to-one to the elements of a transversal of $\overline{\mathrm{Aut}}_K(G)$ in $\mathrm{Aut}(G/K)$ and this yields the desired result.

Theorem 1 translates to an effective method to enumerate the groups of order mp for fixed m and arbitrary prime $p \nmid m$:

1) Let $D = (d_1,\ldots,d_k)$ be the list of divisors of m, with $d_1 = 1$.

2) For all groups G in $\mathscr{L}_m$ determine $w(G)$ with respect to D.

3) Using the values in (2), determine $w_{d_1}(m),\ldots,w_{d_k}(m)$.

4) Determine the (finite) set π of those prime divisors of $(d_2-1)\cdots(d_k-1)$ that do not divide m.

5) For each $p \in \pi$ determine the number a_p of groups of order mp without normal Sylow p-subgroups (for example, using the Frattini extension method and the construction of non-solvable groups).

6) Define $a_p = 0$ if $p \notin \pi$.

7) Given an arbitrary prime p with $p \nmid m$, it now follows that

$$|\mathscr{L}_{mp}| = a_p + \sum_{\substack{i \in \{1,\ldots,k\} \\ \text{with } d_i \mid (p-1)}} w_{d_i}(m).$$

Note that this method can be adapted readily to count solvable and non-solvable groups separately and we use this frequently in applications.

4 Recent improvements to implementations in GAP

Many of the above algorithms rely on effective methods to determine automorphism groups and to decide isomorphism. Here we exhibit various improvements to the existing methods for these purposes. We discuss automorphisms and isomorphisms in the following two subsections and we note that all exhibited improvements will be made public with GAP 4.9.

4.1 Automorphism groups

There are various methods known to determine automorphism groups. For finite p-groups we use the method by Eick, Leedham-Green & O'Brien [13] as implemented in the GAP package [14], for finite solvable groups we use the method by Smith [27], and for finite non-solvable groups we use the method by Cannon & Holt [9]. Smith's method is implemented in the GAP library. This implementation has recently been improved by the third author and it has been combined with an implementation of the method by Cannon & Holt [9].

In the remainder of this subsection, we discuss the recent improvements to the GAP implementation of Smith's method. Let G be a finite solvable group. Smith's method uses induction along a characteristic series of G with elementary abelian factors. Let M by a characteristic elementary abelian subgroup of G of order p^d, say. Then there is a natural homomorphism

$$\varphi : \mathrm{Aut}(G) \to \mathrm{Aut}(G/M) \times \mathrm{Aut}(M).$$

By induction, we assume that $\mathrm{Aut}(G/M)$ is given. Note that $\mathrm{Aut}(M) \cong \mathrm{GL}(d,p)$. The principal idea of Smith's method is to determine $\mathrm{Aut}(G)$ via determining the kernel and image of φ. The kernel of φ is naturally isomorphic to $Z^1(G/M,M)$ and can be determined readily. The image of φ can be described by certain stabilizer calculations; these stabilizer calculations are the main bottlenecks of the method.

One idea towards reducing the bottlenecks is the following. Instead of starting a stabilizer computation with the full direct product $\mathrm{Aut}(G/M) \times \mathrm{Aut}(M)$, we determine *a priori* a subgroup $D \leq \mathrm{Aut}(G/M) \times \mathrm{Aut}(M)$ with $\mathrm{im}(\varphi) \leq D$ and then use D instead of $\mathrm{Aut}(G/M) \times \mathrm{Aut}(M)$. For example, a subgroup D can be determined as the stabilizer of each group in a collection of characteristic subgroups of G. This often breaks a single stabilizer calculation into a sequence of smaller calculations and thus reduces the bottleneck of the overall method.

Using characteristic subgroups is particularly helpful to reduce $\mathrm{Aut}(M)$. In this case the stabilizer of each group in a collection of characteristic subgroups of M in $\mathrm{Aut}(M)$ translates to the stabilizer of a collection of invariant subspaces of $\mathbb{F}_p^d$ in $\mathrm{GL}(d,p)$. This can be determined readily via the method described by Schwingel [24]. We implemented this in GAP and use it in combination with Smith's method.

We exhibit a second idea towards reducing bottlenecks. Let $D \leq \mathrm{Aut}(G/M) \times \mathrm{Aut}(M)$ with $\mathrm{im}(\varphi) \leq D$. Then D acts naturally on the set of homomorphism $G/M \to M$. Let σ denote the homomorphism arising from the conjugation action of G/M on M. One step in Smith's method is to determine the stabilizer in D of σ. We first determine a permutation representation of D related to the action on homomorphisms and then use the highly effective permutation group machinery of GAP to determine the desired stabilizer.

4.2 Isomorphisms

In this section we discuss the GAP implementation of the method of Cannon & Holt [9] to decide if two finite groups G and H are isomorphic. We first determine various invariants of G and H to have a fast initial check for non-isomorphism.

The method of Cannon & Holt uses induction along a fully invariant series through G and H. In each induction step it decides isomorphism and computes the automorphism group of the considered quotient.

Two groups G and H are isomorphic if and only if there exists $\alpha \in \mathrm{Aut}(G \times H)$ with $G^\alpha = H$. This translates an isomorphism test to an automorphism group calculation. Note that it is not necessary for this approach to determine the full automorphism group of $G \times H$: if G and H are isomorphic, then $\mathrm{Aut}(G \times H)$ contains a subgroup $W \cong \mathrm{Aut}(G) \wr C_2$ and G and H are conjugate in W.

Further, with this method it is frequently useful to determine a collection of fully invariant subgroups of G and H *a priori* and to use these subgroups to reduce the calculation, since a fully invariant subgroup of G (such as, for example, G', $\mathrm{Fit}(G)$ or $Z(G)$) has to map onto the corresponding subgroup of H and thus our aim is to determine $\alpha \in W$ that maps these pairs of subgroups onto each other.

5 The groups of order at most 20 000

In this section we describe how we enumerated or constructed the groups of order at most 20 000 with few exceptions.

Nilpotent groups: We have constructed these as direct products of p-groups. The groups of order dividing p^7 have been determined by Newman, O'Brien & Vaughan-Lee [18, 22]. The groups of order dividing 2^9 have been constructed by Eick & O'Brien [15, 20] who also enumerated the groups of order 2^{10}. The groups of order 3^8 have been determined by Vaughan-Lee [30]. Hence the nilpotent groups of order n are available for all $n \in \{1,\ldots,20\,000\}$ except for those n divisible by 2^{10} or 3^9; and the nilpotent groups of order divisible by 2^{10}, but not divisible by 2^{11}, can be enumerated.

Solvable, non-nilpotent groups: We have used the Frattini extension method or the solvable group construction to determine these groups. The Frattini extension method in combination with an improved isomorphism test for solvable groups has been used for the vast majority of orders in the range up to 20 000. The only exception are the groups of order $2^8 \cdot 3^2 = 2\,304$ which were constructed with the solvable group construction method. Further, we used the method of Section 3 to enumerate groups of certain orders. Among the orders n in the range at most 20 000 there are 19 733 orders of the form $m \cdot p$ with p a prime that does not divide m. We applied the method of Section 3 to a significant range of these orders. In particular, we enumerated the groups of order $2^9 \cdot p$ for p an odd prime with this approach.

Non-solvable groups: We have used the combination of the cyclic extension method with the limited version of Archer's $Z\phi$ method to construct these groups. We note that there are 448 orders in the range of orders at most 20 000 for which non-solvable groups exist. For example, we determined 99 926 non-solvable groups of order $7\,680 = 2^9 \cdot 3 \cdot 5$, and counted that there are more than 8 279 000 non-solvable groups of order $15\,360 = 2^{10} \cdot 3 \cdot 5$.

6 Open cases and challenges

We first discuss enumerations of groups before we consider explicit constructions.

6.1 Enumeration

There are 39 orders in the range at most 20 000 for which we have not (yet?) enumerated the groups of these orders. Note that in all but one case, order $15\,360 = 2^{11} \cdot 3 \cdot 5$, the non-solvable groups have been enumerated successfully. Thus, the following discussion is primarily concerned with solvable groups.

First case. Let $E_1 = \{n \in \{1, \ldots, 20\,000\} \mid 2^{10} \mid n \text{ or } 3^9 \mid n\}$. Then E_1 contains 20 orders. For these 20, the nilpotent groups of each order are not explicitly constructed, let alone the non-nilpotent groups. Using the methods in [15], one can determine that there are 4 896 600 938 groups of order 3^9 and exponent-3 class 2. Further, it is known that there are 49 487 365 422 groups of order 2^{10}. These numbers of groups are so large, that the enumeration of groups of orders in E_1 appears to be infeasible. Just to give an idea of the problems that will arise in trying to address this case, we note that the methods of [15] can be used to determine that there are 1 774 274 116 992 170 groups of order 2^{11} and exponent-2 class 2. These methods are available as part of the GAP package [14].

Second case. Let E_2 the set of those $n \in \{1, \ldots, 20\,000\}$ satisfying that $2^9 \cdot p$ is a proper divisor of n for some $p \in \{3,5,7\}$. There are 18 orders in E_2. There are over 400 000 000 groups for each of the orders $2^9 \cdot p$ with $p \in \{3,5,7\}$. Hence, again, these numbers are so large, that the enumeration of groups of orders in E_2 appears to be infeasible.

Third case. Let $E_3 = \{n \in \{1, \ldots, 20\,000\} \mid (2^8 \cdot p^2) \mid n \text{ for some } p \in \{3,5,7\}\}$. There are 12 orders in E_3. These orders are difficult cases for the construction of solvable groups via the Frattini extension method. We have determined the 15 756 130 groups of order $2^8 \cdot 3^2$ using the solvable group construction. This order is an exception in the set E_3.

Exceptional cases. Six orders remain which are not in $E_1 \cup E_2 \cup E_3$ and the construction of the groups of these orders is an open problem. We list these orders in the following table. The nilpotent groups of each of these orders are determined. Where known, we exhibit in the table the numbers of nilpotent, solvable and non-solvable groups.

n	# nilpotent	# solvable	# non-solvable
$8\,748 = 2^2 \cdot 3^7$	18 620	not known	0
$10\,368 = 2^7 \cdot 3^4$	34 920	not known	0
$13\,122 = 2 \cdot 3^8$	1 396 077	not known	0
$16\,000 = 2^7 \cdot 5^3$	11 640	not known	0
$17\,496 = 2^3 \cdot 3^7$	46 550	not known	0
$18\,816 = 2^7 \cdot 3 \cdot 7^2$	4 656	not known	387

6.2 Construction

As observed in the previous paragraph, for all but 39 orders at most 20 000 we have enumerated the numbers of groups of these orders. For the vast majority of these orders we have also determined isomorphism type representatives explicitly: more precisely, there are 34 orders for which we have enumerated the corresponding groups only, but did not construct them. This includes the order 2^{10} for which the groups have been enumerated using the methods in [15].

For another 32 of these orders, we have used the approach exhibited in Section 3 to enumerate the groups of these orders. These orders are of the form $2^9 p$ for p an odd prime, of the form $2^8 pq$ for $p \in \{3,5,7\}$ and q a prime different from 2 and p, of the form $2^7 3^2 p$ for p a prime different from 2 and 3, and the orders

$$8\,640 = 2^6 \cdot 3^3 \cdot 5, \qquad 9\,600 = 2^7 \cdot 3 \cdot 5^2, \qquad 13\,440 = 2^7 \cdot 3 \cdot 5 \cdot 7,$$
$$16\,320 = 2^6 \cdot 3 \cdot 5 \cdot 17, \qquad 17\,280 = 2^7 \cdot 3^3 \cdot 5, \qquad 19\,440 = 2^4 \cdot 3^5 \cdot 5.$$

Finally, we counted the groups of order $12\,500 = 2^2 \cdot 5^5$ using a modified version of the method described in Section 3, by exploiting that these groups always admit a normal Sylow 5-subgroup.

For all other 19 927 orders in the range of orders at most 20 000, we have explicitly determined the groups of the corresponding orders, unless they are already available in the SmallGroups library [5]. The resulting groups will be made available as a package for GAP.

7 Reliability of the data

It is important to cross-check the computed data for group constructions and enumerations. One very useful way for doing this is to determine or enumerate the

groups of a certain order in two different ways. We have done this in many cases. In all of them the results of the different methods agree with each other.

We computed non-solvable groups using both the cyclic extension method and the limited version of Archer's $Z\phi$ method whenever Archer's method applies. Additionally, we used the method of Section 3 to obtain an independent enumeration of the groups whenever the order is of the type mp with p prime and m coprime to p and we used different types of such factorisations of the order when possible. Out of the 447 orders admitting non-solvable groups, we enumerated 441 with at least two different methods. This leaves only six cases which were not cross-checked.

For the solvable groups, we employed two methods: the Frattini extension method, as well as the enumeration approach from Section 3. In the range of order at most 20 000, the SmallGroups library [5] already covers 17 903 orders. Of the remaining 2 097 orders, we enumerated 1 875 orders with both methods, 183 orders with only one method, and 39 orders remain open, see Section 6.

References

1. C. Archer. The extension problem and classification of nonsolvable groups. PhD Thesis, Université Libre de Bruxelles, 1998.
2. H. U. Besche and B. Eick. Construction of finite groups. *J. Symb. Comput.*, 27:387 – 404, 1999.
3. H. U. Besche and B. Eick. *GrpConst - Construction of finite groups*, 1999. A refereed GAP 4 package, see [29].
4. H. U. Besche and B. Eick. The groups of order $q^n \cdot p$. *Comm Alg.*, 29(4):1759 – 1772, 2001.
5. H. U. Besche, B. Eick, and E. O'Brien. *SmallGroups - a library of groups of small order*, 2005. A GAP 4 package; Webpage available at www.icm.tu-bs.de/ag_algebra/software/small/small.html.
6. H. U. Besche, B. Eick, and E. A. O'Brien. The groups of order at most 2000. *Electronic Research Announcements of the AMS*, 7:1 – 4, 2001.
7. H. U. Besche, B. Eick, and E. A. O'Brien. A millenium project: constructing small groups. *Internat. J. Algebra Comput.*, 12:623 – 644, 2002.
8. S. Blackburn, P. Neumann, and G. Venkataraman. *Enumeration of finite groups*. Cambridge University Press, 2007.
9. J. J. Cannon and D. F. Holt. Automorphism group computation and isomorphism testing in finite groups. *J. Symb. Comput.*, 35:241 – 267, 2003.
10. A. Cayley. On the theory of groups, as depending on the symbolic equation $\theta^n = 1$. *Philos. Mag.*, 4(7):40 – 47, 1854.
11. J. Conway, H. Dietrich, and E. O'Brien. Counting groups: gnus, moas and other exotica. *Math. Intelligencer*, 30:6–15, 2008.
12. B. Eick and M. Horn. The construction of finite solvable groups revisited. *J. Algebra*, 408:166–182, 2014.
13. B. Eick, C. R. Leedham-Green, and E. A. O'Brien. Constructing automorphism groups of p-groups. *Comm. Alg.*, 30:2271 – 2295, 2002.
14. B. Eick and E. O'Brien. *AutPGrp - Computing the automorphism group of a p-group, Version 1.8*, 2016. A refereed GAP 4 package, see [29].
15. B. Eick and E. A. O'Brien. Enumerating p-groups. *J. Austral. Math. Soc.*, 67:191 – 205, 1999.

16. D. Holt and W. Plesken. *Perfect groups*. Clarendon Press, 1989.
17. M. Horn and B. Eick. *GroupExt - Constructing finite groups*, 2013. A GAP 4 package, see [29].
18. 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. Alg.*, 278:383 – 401, 2003.
19. E. O'Brien. *ANUPQ - the ANU p-Quotient algorithm*, 1990. Also available in MAGMA and as GAP package.
20. E. A. O'Brien. *The groups of order dividing* 256. PhD thesis, Australian National University, Canberra, 1988.
21. E. A. O'Brien. The p-group generation algorithm. *J. Symb. Comput.*, 9:677 – 698, 1990.
22. E. A. O'Brien and M. R. Vaughan-Lee. The groups with order p^7 for odd prime p. *J. Algebra*, 292(1):243–258, 2005.
23. L. Pyber. Group enumeration and where it leads us. In *European Congress of Mathematics, Vol. II (Budapest, 1996)*, volume 169 of *Progr. Math.*, pages 187–199. Birkhäuser, Basel, 1998.
24. R. Schwingel. Two matrix group algorithms with applications to computing the automorphism group of a finite p-group. PhD Thesis, QMW, University of London, 2000.
25. J. K. Senior and A. C. Lunn. Determination of the Groups of Orders 101-161, Omitting Order 128. *Amer. J. Math.*, 56(1-4):328–338, 1934.
26. J. K. Senior and A. C. Lunn. Determination of the Groups of Orders 162-215 Omitting Order 192. *Amer. J. Math.*, 57(2):254–260, 1935.
27. M. J. Smith. *Computing automorphisms of finite soluble groups*. PhD thesis, Australian National University, Canberra, 1995.
28. D. Taunt. Remarks on the isomorphism problem in theories of construction of finite groups. *Proc. Cambridge Philos. Soc.*, 51:16 – 24, 1955.
29. The GAP Group. GAP – *Groups, Algorithms and Programming, Version 4.4*. Available from http://www.gap-system.org, 2005.
30. M. Vaughan-Lee and B. Eick. *SglPPow – Database of certain p-groups*, 2016. A GAP 4 package, see [29].