A millennium project: constructing small groups

Hans Ulrich Besche, Bettina Eick and E.A. O'Brien

Abstract

We survey the problem of constructing the groups of a given finite order. We provide an extensive bibliography and outline practical algorithmic solutions to the problem. Motivated by the millennium, we used our algorithms to construct the groups of order at most 2000; we report on this calculation and describe the resulting group library.

1 Introduction

The construction of the groups of a given finite order has a long history; it was initiated by Cayley in 1854. The central task is to provide 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 have the same isomorphism type. The primary difficulty is the reduction to isomorphism types; it is comparatively easy to give a complete list.

Historically, the approaches to this problem involved a large number of hand-computations and case distinctions, and focused on very specific properties of the groups. They were consequently *ad-hoc* in nature, and many contained significant errors. We provide an extensive bibliography in Section 2.

More recently, practical algorithms have been developed to construct the groups of a given order. These include:

- The p-group generation algorithm of Newman (1977) and O'Brien (1990).
- The p-group enumeration methods of Eick & O'Brien (1999).
- The coprime split extension algorithm of Besche & Eick (1999a, 2000).
- The Frattini extension method of Besche & Eick (1999a, 2000).
- Algorithms to construct insoluble groups.

While these methods rely on group-theoretic properties, they are inherently *general-purpose* and their results appear reliable. We outline the main features of each algorithm in Section 3.

Motivated by the millennium, we used our implementations to enumerate 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. We report on this calculation in Section 4 and comment on its reliability.

The resulting catalogue of groups of order at most 2000 (excluding those of order 2^{10}) forms part of the electronic Small Groups library. This library is available on the WEB and is distributed with the computer algebra systems GAP (The GAP Team, 1999) and Magma (Bosma, Cannon and Playoust, 1997). The connection to such systems is particularly useful, since they permit effective searching and further study of the groups. We describe the library in Section 5. An important requirement, centrally related to accuracy, is the ability to identify a given group in the library. We consider this problem in Section 6.

While our algorithms (and their publicly-available implementations) can be used to extend existing determinations, we believe that the new challenge is to construct "generic" groups – for example, those whose orders factorise in a certain way. The Small Groups library includes those groups whose orders have at most 3 prime divisors; Besche & Eick (2000) present an algorithm to determine the groups of order $p^n \cdot q$ for arbitrary distinct primes p, q.

The development of group-theoretic database facilities (encompassing significant amount of stored data and a query language) would assist effective exploration of the groups; a prototype database for the groups of order dividing 256 was developed by Butler, Iyer & O'Brien (1993).

2 Historical background

Here we review the history of group construction. This material incorporates and updates earlier work of O'Brien & Short (1988).

We discuss the work loosely sorted by increasing order, and provide information on each order in chronological order. No claims are made about the accuracy of the referenced work, except where explicitly stated, or on the comprehensiveness of the references.

The term "enumeration" is used to describe the counting of groups; "determination" indicates that presentations of the groups are obtained; "classification" indicates that the groups are organised according to some criteria. The symbols p, q, r, and s denote distinct primes.

Cayley (1854, 1859) determined the cyclic groups and the groups of order 4, 6, and 8. Netto (1882, pp. 133-137) determined the groups of order p^2 and those of order pq. Kempe (1886) listed the groups of order 8 and, inaccurately, those of order 12. The groups of order at most 12 were correctly listed by Cayley (1889).

The groups of order p^3 were independently determined by Cole & Glover (1893), Hölder (1893), and Young (1893). The groups of order p^2q and pqr were listed by Cole & Glover (1893) and Hölder (1893). The work of the former on the groups of order

p^2q was corrected by Hölder (1895a). Miller (1921a, 1921b) wrongly claimed that Hölder's work was inaccurate; a new determination was carried out by Lin (1974). The groups of order p^4 were determined by Hölder (1893) and Young (1893). The groups of square-free order were determined by Hölder (1895b); the groups of order $pqrs$ were also determined by Baudet (1918). Levavasseur (1896b) determined the groups of order $8p$; these were independently enumerated by Miller (1896a) who claimed that there are errors in the work of Levavasseur.

Levavasseur (1896a) claimed that there were more than 75 groups of order 32. A list of 51 groups was given by Miller (1896b). When Miller (1936) recalculated the groups of order 32, he obtained only 47. Sophie (1962) provided an explanation for his errors and also verified the correctness of his original list.

Miller (1896b) provided generating sets of permutations for the groups of order less than 48. Burnside (1897, pp. 105-108) determined the groups of order 60.

The groups of order p^5 were listed by Bagnera (1898). Miller (1899) pointed out errors for the groups of order 2^5 which were corrected by Bagnera (1899). A new list was provided by de Séguier (1904, §154-159); Schreier (1926) published a list for $p \geq 5$. Bender (1927) published a list showing errors in Bagnera's calculations for the groups of order 3^5 but omitted a maximal class group which was included by Blackburn (1958). James (1968, 1980) provided a correct list of the groups of order 3^5.

The groups of order 48 and $2p^3$ were enumerated by Miller (1898) and those of order p^3q were determined by Western (1899). The groups of order p^2q^2 were initially determined by Le Vavasseur (1899a, 1902) and later by Lin (1974). They were also enumerated by Laue (1982, pp. 214-243). The results of Lin and Laue are identical, although Lin's summary has a counting error.

The groups of order $16p$ were determined by Le Vavasseur (1899b, 1903); Lunn & Senior (1934) claimed that there were errors in his work and enumerated the groups of this order. The groups of order $8p^3$ and $16p^2$ were determined by Nyhlén (1919) (there are known errors in his work for groups of order 216) and those of order $8p^2$ by Zhang (1983). The groups of order 168 were enumerated by Miller (1902); those of order $8pq$ were determined by Wen (1984). Some groups whose orders are products of 6 primes were determined by Malmrot (1925).

Glenn (1906) incorrectly determined the groups of order p^2qr; the number of such groups can be found using the work of Laue (1982, pp. 244-262). The groups of order p^3q^2 were determined by Tripp (1909). Both Nyhlén (1919, p. 37) and Malmrot (1925, pp. 87-88) claim that Tripp's list is incomplete for the groups of order 72 and a list of 50 presentations is provided by Malmrot. In an independent enumeration, Miller (1929) also found 50 groups. An inaccurate enumeration of the groups of order 96 was given by Miller (1930b); Lunn & Senior (1934) enumerated the groups of order $32p$. The groups of order 96 are listed in Laue (1982, pp. 278-296); a corrigendum to this work corrects some errors.

Potron (1904a, 1904b) gave an incomplete list of the groups of order 64. Miller (1930a) claimed that there is a total of 294 groups. A correct list was calculated by P. Hall & Senior in the 1930s and published by M. Hall & Senior (1964). McKay (1969) corrected some of the supplied permutations representations.

The first work on the groups of order p^6, for p an odd prime, is also in Potron (1904a, 1904b). Tordella (1939) described some errors in this work but his work is incomplete. Easterfield (1940) provided presentations for the groups, for $p > 3$, and their classification into isoclinism families. Blackburn (1958) classified the maximal class groups of order p^6. A list of the groups calculated by James (1968) had a number of errors and was incomplete. Küpper (1979) corrected some of these errors. A revised list, incorporating corrections by Keane for groups of order 3^6 and incorrectly the work of Küpper, was published by James (1980). It agreed, in the relevant sections, with Blackburn (1958), and the subclasses of p-groups published by Leong (1974) and Miech (1975). However, it contains a number of serious errors, some of which are documented by Pilyavskaya (1983). A summary of known errors and corrections is given in Newman & O'Brien (1986). The groups of order 3^6 were determined by Baldwin (1987).

A comprehensive listing of presentations and certain properties, in particular the subgroup lattices, of the groups of order at most 100, excluding those of order 64 and 96, was provided by Neubüser (1967). Recent treatments of metacyclic groups include Sim (1994), Liedahl (1996) and Hempel (2000).

In the 1930s, P. Hall determined some of the isoclinism families for the groups of order 128. An inaccurate enumeration of the groups of order 128 was given by Rodemich (1980). An independent determination of these groups was provided by James, Newman & O'Brien (1990). Wilkinson (1988) lists groups of order p^7 and exponent p; see Zbl 651.20025 for comments on known errors. The groups of order 256 were determined by O'Brien (1991).

The groups of order 108, 120, 144, 162, 180, and 200 were enumerated by Lunn & Senior (1934, 1935). The groups of order 180 were determined by Jabber (1941) and Taunt (1948) provided confirmation of his work. Taunt (1955) discussed the construction of soluble groups of cube-free order. Laue (1982, pp. 214-243) enumerated soluble groups of certain orders. Betten (1996) presents an algorithm to construct soluble groups and used it to determine those of order at most 242. Insoluble groups of order less than 960 were listed by Patris-Moreau (1975). The perfect groups of order at most 1 000 000 were determined by Holt & Plesken (1989).

The non-nilpotent groups of order at most 1000 were determined by Besche & Eick (1999a, 1999b). Their work agrees with that of Laue (1982), Betten (1996) and Lunn & Senior (1934, 1935). Eick & O'Brien (1999) enumerated the 10 494 213 groups of order 2^9.

3 Construction and enumeration algorithms

We now provide an overview of our algorithms. Naturally, the techniques depend on inherent group-theoretic structural properties, such as nilpotence and solubility. A central requirement is that the algorithms are practical. Implementations of the algorithms are publicly available in either of GAP or MAGMA.

3.1 The p-group generation algorithm

The p-group generation algorithm is used to determine groups of prime-power order.

The lower exponent-p central series of a p-group G is the descending series of subgroups defined recursively by $P_1(G) = G$ and $P_{i+1}(G) = [P_i(G), G]P_i(G)^p$ for $i \geq 1$. If c is the smallest integer such that $P_{c+1}(G) = 1$, then G has exponent-p class c.

The p-group generation algorithm proceeds by induction down the lower exponent-p central series. A single iteration determines up to isomorphism all *immediate descendants* of a given p-group G of exponent-p class c: those groups H of exponent-p class $c+1$ such that $H/P_c(H) \cong G$.

Observe that $P_1(G) = \Phi(G)$ the Frattini subgroup of G; if the elementary abelian group $G/P_1(G)$ has order p^d, then G is a d-generator group. Clearly, G can be constructed by iterating the inductive step and so all d-generator p-groups can be obtained as extensions of the elementary abelian group of order p^d.

In more detail, the construction of the immediate descendants of a p-group G of exponent-p class c proceeds as follows. As a first step, we determine the maximal central, elementary abelian Frattini extension of G. This extension G^* is the *p-covering group* of G and every immediate descendant of G is a quotient of G^*.

By definition, G^* has a normal subgroup M where $G^*/M \cong G$ and M is elementary abelian, central and contained in the Frattini subgroup of G^*. The subgroup M is the *p-multiplicator* of G. Further, G^* has exponent-p class at most $c+1$ and $N := P_{c+1}(G^*) \leq M$ is the *nucleus* of G. If U is a supplement of N in M, then G^*/U is an immediate descendent of G.

Moreover, $Aut\,(G)$, the automorphism group of G, induces a linear action on M. Two immediate descendants of G are isomorphic if and only if their corresponding supplements are contained in the same orbit under $Aut\,(G)$. Hence, to solve the isomorphism problem, we determine orbits of supplements to N in M under the induced action of $Aut\,(G)$. As a by-product, we also obtain the automorphism groups of the immediate descendants, which permits iteration.

A description of the algorithm appears in Newman (1977) and in O'Brien (1990).

3.2 Enumerating p-groups

In the p-group generation algorithm, the isomorphism problem for immediate descendants of a p-group G is solved by computing orbits. If we want simply to count the number of immediate descendants, we need only determine the *number* of such orbits.

We use the Cauchy-Frobenius Lemma (see, for example, Robinson (1996, p. 42)) for this purpose. Let D be the set of supplements to N in M and $A = Aut\,(G)$ the acting group. Then

$$\#\text{ orbits in } D \text{ under } A \;= \frac{1}{|A|}\sum_{a\in A} Fix_a(D),$$

where $Fix_a(D)$ is the number of fixed points of a in D. Hence we can instead compute the number of fixed points in D for each $a \in A$. Clearly, we can restrict to conjugacy class representatives of A.

Let D_d be the set of supplements U of dimension d in M. We view the elementary abelian p-group M as a vector space over $\mathbf{F}_p$ and introduce $T = M \otimes L$ where L is a d-dimensional vector space over $\mathbf{F}_p$. Then elements of D_d correspond to certain elements of T via

$$\tau \ : \ D_d \ \to \ T \ : \ \langle u_1, \ldots, u_d \rangle \ \mapsto \ \sum_{i=1}^{d} u_i \otimes l_i.$$

The group $A \times \mathrm{GL}(d,p)$ acts componentwise on T and, moreover, the action of A on D_d corresponds to the action of $A \times \mathrm{GL}(d,p)$ on the image of τ. It is now significantly easier to determine fixed points: $A \times \mathrm{GL}(d,p)$ acts as a matrix group on the vector space T and thus the set of fixed elements in T under action of $r \in A \times \mathrm{GL}(d,p)$ can be computed as the nullspace of $r - 1$.

In applying this enumeration variant of p-group generation, we face two practical problems: a comparatively large group $A \times \mathrm{GL}(d,p)$ acts, and we must determine the elements of T in the image of the map.

Eick & O'Brien (1999) address these problems as part of a cohomological-based version of the p-group generation algorithm. They also present a particularly efficient algorithm for the special case where G is elementary abelian, obtaining in effect a concrete realisation of the Higman (1960) exponent-p class 2 calculation.

3.3 Coprime split extensions

We introduce a method to determine up to isomorphism all groups of order $r \cdot s$ with normal Hall r-subgroup and $\gcd(|r|, |s|) = 1$. It takes as input a list of the groups of orders r and s. A special case appears in Besche & Eick (1999a, §5); a similar approach was outlined by Taunt (1955).

Let G be a group of order $r \cdot s$ with a normal Hall r-subgroup. Then $G = R \rtimes S$ where $|R| = r$ and $|S| = s$. The isomorphism type of G depends on the isomorphism types of R and S and the action of S on R. If we assume R and S are given, it remains to determine a list of actions of S on R such that the resulting list of isomorphism types is complete and irredundant.

Each action of S on R corresponds to a homomorphism $\psi : S \to Aut(R)$. Let K be its kernel; that is, $K = C_S(R)$. Since R and S have coprime order, $U = Im(\psi)$ intersects trivially with $Inn(R)$ and thus can be considered as a subgroup of $Out(R)$. Thus, $S/K \cong U \cong UInn(R)/Inn(R) \leq Out(R)$ and hence ψ corresponds to a diagonal subgroup D in $Out(R) \times S$ such that $D \cap Out(R) = 1$ and D covers S. Figure 1 illustrates this.

The orbits of such a diagonal subgroup D under the natural componentwise action of $Out(R) \times Aut(S)$ on $Out(R) \times S$ are in one-to-one correspondence with a set of actions of S on R such that the resulting list of isomorphism types of groups $R \rtimes S$ is both complete and irredundant.

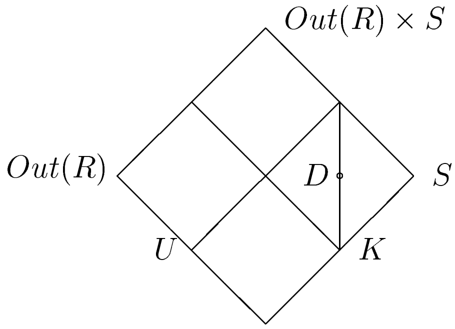

Figure 1: Coprime split extension method

Eick (1997) presents a practical method to compute subdirect products up to conjugacy. Its application here translates into the following algorithm.

1. Determine up to conjugacy all subgroups U of order dividing s in $Out(R)$.
2. For each U in the resulting list, determine up to conjugacy under $Aut\,(S)$ the normal subgroups K of S with $S/K \cong U$.
3. For each $K \leq S$ with $S/K \cong U$, determine the diagonal subgroups in $U \times S/K$ up to conjugacy under $N_{Out(R)}(U) \times Stab_{Aut\,(S)}(K)$.

Step 3 can be realised by a double coset computation in $V \setminus Aut\,(U)\ /\ W$ where $V \leq Aut\,(U)$ is induced by action of $N_{Out(R)}(U)$ on U and $W \leq Aut\,(S/K) \cong Aut\,(U)$ is obtained by the action of $Stab_{Aut\,(S)}(K)$ on S/K.

The algorithm must compute automorphism groups and isomorphisms, usually demanding calculations. However, in circumstances where these calculations are possible, this method is more efficient than the Frattini extension method of Section 3.4, since it solves the isomorphism problem by computing orbits. In particular, if S is a p-group, its automorphism group can be computed efficiently using an algorithm of Eick, Leedham-Green & O'Brien (2000); also if R has order q, q^2 or qr, then $Out(R)$ is small.

3.3.1 A variation for generic groups

Besche & Eick (1999a) use the coprime split extension method to determine those groups of order $p^n \cdot q$, for given primes $q \neq p$, having a normal Sylow q-subgroup.

Besche & Eick (2000) generalise this approach to obtain these groups for all primes $q \neq p$ simultaneously. Following our earlier notation, let $r = q$ and $s = p^n$. Then R is cyclic of order q and $Aut\,(R)$ is cyclic of order $q - 1$. Therefore the coprime split extension approach can be applied generically, without specifying q.

The groups of order $p^n \cdot q$ without normal Sylow q-subgroup exist for finitely many primes only and can be determined using the Frattini extension method of Section 3.4.

3.4 The Frattini extension method

The Frattini extension method can be used to determine certain or all soluble groups of a given order. The algorithm is described in Besche & Eick (1999a); an extension is presented in Besche & Eick (2000).

Recall that the Frattini subgroup $\Phi(G)$ is the intersection of all maximal subgroups of the finite group G. A group H is a *Frattini extension* of G if there exists $N \lhd H$ with $N \leq \Phi(H)$ such that $H/N \cong G$. Thus each group G is a Frattini extension of its Frattini factor $G/\Phi(G)$.

We construct the groups of order n as follows.

(1) Determine up to isomorphism candidates F for the Frattini factors of the desired groups of order n.

(2) For each candidate F:

   (a) Compute the Frattini extensions of order n of F.

   (b) Reduce the resulting list of extensions to isomorphism type representatives.

The construction of candidates for the Frattini factors F relies on the work of Gaschütz (1953). Let G be a soluble group of order n and $F = G/\Phi(G)$ its Frattini factor. Then $|F| \mid n$ and each prime divisor of n divides $|F|$. Further, the socle $Soc(F)$ is a direct product of elementary abelian groups and has a complement K in F. The socle complement K acts faithfully on $Soc(F)$ and each Sylow p-subgroup of $Soc(F)$ is a semisimple $\mathbf{F}_pK$-module.

Thus we determine candidates for the Frattini factors F of the desired groups by considering all direct products of elementary abelian groups of order dividing n as possible socles S for F. We then construct up to conjugacy all subgroups K of $Aut\,(S)$ which have suitable order and act semisimply on S. Finally, we obtain the desired candidates F as $S \rtimes K$.

In step (2a), we compute Frattini extensions of a candidate F using a recursive approach. Let H be a Frattini extension of F where $|H| \mid n$. Then each Frattini extension of H is also a Frattini extension of F. Let p be a prime dividing $n/|H|$. We compute the irreducible $\mathbf{F}_pH$-modules M up to equivalence and for each module M calculate $H^2(H, M)$. Since M is irreducible, the non-trivial elements of $H^2(H, M)$ correspond to the equivalence classes of Frattini extensions of H by M.

Thus, we obtain each Frattini extension of F of order n at least once. However, the iterated computation of minimal Frattini extensions usually produces redundancy, since equivalence of extensions is weaker than isomorphism. We use an action of $Aut\,(H)$ on $H^2(H, M)$ to eliminate some of this redundancy. Then, in step (2b), we reduce the list of groups to representatives of distinct isomorphism types in two stages: we first apply an efficient random method to search for isomorphic copies and then verify the irredundancy of the remaining groups by determining distinguishing invariants. This isomorphism reduction is described in Besche & Eick (2000).

Various group-theoretic properties are determined by the Frattini factor of a group. Thus we can use the algorithm to construct groups with certain properties only, by restricting the choice of the candidates for the Frattini factors. In particular, we can construct non-nilpotent groups or groups without normal Hall subgroups only.

3.5 Constructing insoluble groups

Let G be a finite group with *soluble residuum* N: namely, N is the smallest normal subgroup of G with G/N soluble. Then N is a perfect group. A catalogue of perfect groups of order at most one million was determined by Holt & Plesken (1989).

Assume we wish to determine the insoluble groups G of order n with given soluble residuum N. We distinguish between two cases.

(1) If $Z(N) = 1$, then G can be determined efficiently using a subdirect product computation.

(2) If $Z(N) > 1$, then we apply the (well-known) cyclic extension method and subsequently reduce to isomorphism type representatives.

In case (1), we assume that we know a list of soluble groups S of order $n/|N|$. For each S, we construct up to isomorphism the groups G with soluble residuum N and $G/N \cong S$. Let $\psi : G \to Aut\,(N)$ be the natural conjugation action of G on N and let U be the image of ψ. Since N is centre-free, $N \cong Inn(N) \leq U \leq Aut\,(N)$. Alternatively, we can view G as a subdirect product in $U \times S$ with amalgamated factor groups $U/Inn(N) \cong S/C_S(N)$.

Moreover, $Aut\,(N) \times Aut\,(S)$ acts componentwise on $Aut\,(N) \times S$. To construct the subdirect products $G \leq U \times S \leq Aut\,(N) \times S$ up to isomorphism, we determine orbit representatives of such subgroups under the action of $Aut\,(N) \times Aut\,(S)$ on $Aut\,(N) \times S$. These can be obtained efficiently using the subdirect product construction of Eick (1997) and the resulting algorithm is similar to that outlined in Section 3.3.

In case (2), we use a simpler approach to construct the desired groups. Assume that H is a group with soluble residuum N and $|H| \mid n$. Then G is a *cyclic extension* of H if $H \lhd G$ and G/H cyclic. To determine cyclic extensions of H, we compute $Aut\,(H)$ and loop over its conjugacy classes of cyclic subgroups. Clearly, we obtain all groups of order n with soluble residuum N by iterating this construction.

However, this approach does not solve the isomorphism problem. Hence, after each cyclic extension iteration, we reduce to isomorphism type representatives. Usually, this is the most difficult part in this computation: we use the random isomorphism test of Section 3.4 followed, if necessary, by the method of Hulpke (1996).

In practice, we use this approach only in the case where G/H is cyclic of prime order. The cyclic extension method was employed by Laue (1982) and Betten (1996). An alternative approach for case (2) was introduced by Archer (1998).

4 The groups of order at most 2000

The groups whose orders have at most 3 prime divisors were determined by Hölder (1893). We constructed the groups for the remaining 640 orders using the methods of Section 3.

1. The groups of order 2^{10} and exponent-p class 2 were enumerated using the algorithm of Section 3.2. All other p-groups were constructed using the p-group generation algorithm.

2. The nilpotent groups were obtained as direct products of p-groups.

3. The non-nilpotent groups G of order $p^n \cdot q$ for primes $p \neq q$ such that G has a normal Sylow subgroup were constructed using the coprime split extension method.

4. The non-nilpotent groups of orders $2^7 \cdot 3^2$ and $2^7 \cdot 3 \cdot 5$ having a normal 2-complement were constructed using the coprime split extension method.

5. All remaining soluble, non-nilpotent groups were constructed using the Frattini extension method.

6. The insoluble groups were obtained using the methods of Section 3.5.

In Appendix A, we record the numbers of groups of order at most 2000; the resulting library of groups is discussed in Section 5.

In practice, the difficulty experienced in constructing the groups of order n is determined by the number $f(n)$ of groups of that order. Pyber (1993) shows that $f(n) \leq n^{(2/27+o(1))\mu(n)^2}$, where $\mu(n)$ is the largest exponent in the prime-power factorisation of n. While this is an upper bound, we expect that the orders divisible by prime-powers of large exponent will be the hardest cases for the construction algorithms. We record the most difficult orders and the corresponding number of groups in Table 1.

The enumeration of the groups of order 2^{10} and exponent-p class 2 took approximately 100 seconds using our MAGMA V2.5 implementation on a Sun UltraSPARC Enterprise 4000 server. The remaining groups of order 2^{10} and all groups of order 2^9 were determined using p-group generation; here we needed the extension of O'Brien (1991). We also used our GAP implementation of the cohomology variation of p-group generation to check some of these calculations.

For the groups of order $2^n \cdot p$ where p is an odd prime, it was necessary to use the coprime split extension method for the groups with a normal Sylow subgroup and restrict the Frattini extension method to the remaining groups. As one example, the determination of the groups of order $2^9 \cdot 3$ with normal Sylow subgroup took approximately 663 hours and the remaining 96 437 groups of this order were constructed in 461 hours; in both cases we used our GAP implementations under Linux.

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

Table 1: The number of groups for selected orders

The coprime split extension method was also essential in determining the groups of orders $2^7 \cdot 3^2$ and $2^7 \cdot 3 \cdot 5$. (These orders motivated the generalisation of the cyclic split extension method of Besche & Eick (1999a) to the coprime split extension method.)

4.1 Reliability of the data

The data was generated electronically, without intermediate hand computations. Hence the primary error sources are possible programming errors in our implementations or in the underlying computer algebra systems. Our implementations are publicly available and thus can be inspected. We performed systematic cross-checks on the data in order to limit the possibility of programming errors. Here we record some of these.

The groups of order at most 100 agree with the catalogues of Hall & Senior (1964), Neubüser (1967), Laue (1982), Betten (1996), and the enumerations of Lunn & Senior (1934, 1935).

For a large number of orders having at most 3 prime factors, we constructed (and cross-checked) the corresponding groups using both the descriptions of Hölder and the Frattini extension method.

We determined those groups having a normal Hall subgroup for various orders – including 192, 320, 448, 576, and 960 – in two ways: by the coprime split extension method and by the Frattini extension method.

The non-nilpotent groups of order at most 1000 were constructed using independent implementations in GAP 3 and GAP 4 of each of the Frattini extension and the coprime split extension methods.

The groups of order 256 and 512 were determined using the p-group generation algorithm and were independently enumerated using the methods of Section 3.2.

The automorphism groups of the groups of order 512 are used both by the coprime split extension method and in the enumeration of the groups of order 2^{10}. These automorphism groups were first obtained from p-group generation and later calculated independently using either the algorithm of Eick *et al.* (2000) or a random approach.

As part of the Frattini extension method, we computed invariants of the constructed groups to verify non-isomorphism. Hence we obtain evidence that these parts of the library are irredundant.

5 The Small Groups library

Currently, the Small Groups library contains the following groups:

- The groups whose orders have at most 3 prime divisors.
- The groups of order at most 2000 except 2^{10}.
- The groups of order $p^n \cdot q$ for primes $p \neq q$ where p^n divides 2^8, 3^6, 5^5 or 7^4.

In both GAP and Magma, the groups are readily accessible and additional information about them can be computed. Insoluble groups are returned as permutation groups. Soluble groups are described by power-commutator presentations; these are presentations of the form

$$\begin{aligned}\langle g_1, \ldots, g_n \quad | \quad & g_i^{p_i} = g_{i+1}^{e_{i+1}} \cdots g_n^{e_n} \text{ for } 1 \leq i \leq n \text{ with } 0 \leq e_i < p_i, \\ & [g_j, g_i] = g_{i+1}^{f_{i+1}} \cdots g_n^{f_n} \text{ for } 1 \leq i < j \leq n \text{ with } 0 \leq f_j < p_i \rangle.\end{aligned}$$

5.1 Categories of groups and their internal descriptions

Internally, we store the groups in a compressed format. In selecting the format, we distinguish among four categories of groups.

The *generic groups* whose orders have at most 3 prime divisors are not stored explicitly but are instead defined by functions.

The *split groups* determined using the coprime split extension method are stored using their construction components: the library number of their factors R and S and a description of the operation of S on R.

The Frattini extension method and the p-group generation algorithm both return power-commutator presentations. Each presentation is encoded as a single long integer which effectively describes the exponents of the right-hand side of each relation; the encoding procedure is described in Besche & Eick (1999a). We store this integer for each *encoded group*. For reasons related to the development of the library, the soluble groups of order at most 1000 except 768 are encoded.

The *insoluble groups* are stored using a small generating set for a small-degree permutation representation.

In practice, additional compression is employed to store the groups of some orders efficiently. The resulting Small Groups library is approximately 25 MB in size.

5.2 Organisation of the library

The groups of each order are organised as a sequence. The non-split groups are sorted by increasing library number of their Frattini factor F.

Of course, a group G may equal its Frattini factor F. Recall F is a semidirect product $S \rtimes K$ where S is the Fitting subgroup of F; further, S is a direct product of elementary abelian groups. We sort the Frattini factors F by increasing library number of first S and then the complement K, and, finally, that of the preimage in G of a complement of the Fitting subgroup of $G/\Phi(G)$.

Now we sort those groups G of a fixed order having the same Frattini factor. We use the ordering of Newman & O'Brien (1989) for p-groups. For nilpotent groups we use, recursively, the library numbers of their Sylow subgroups. Otherwise, we sort according to the library number of the Fitting subgroup of G.

For split groups $R \rtimes S$, the construction algorithm dictates the sorting employed: we use the library numbers of R and S and the sequence in which the implementation of the coprime split extension method outputs the possible actions of S on R.

5.3 The development of the library

A precursor to the Small Groups library was released by Newman & O'Brien (1989). It contained encodings for the groups of order dividing 128; later additions included the groups of order 256 and those of order dividing 729.

The 1st edition of the Small Groups library contained the groups of order at most 1000, except 512 and 768, stored as encodings. It incorporated the data of Newman and O'Brien without changes.

For the 2nd edition of the library, we added the generic groups and the groups of orders $2^n \cdot p$ for $n \leq 8$ and p an odd prime. The generic groups replaced the encoded groups of corresponding orders. For the groups of order $2^n \cdot p$ we introduced the split group format, but in this case the original data was incorporated unchanged.

Here, we describe in effect the 3rd edition of the library. While the library may expand in future, we plan no changes to the published parts. It is designed so that it can be expanded easily without affecting existing parts.

6 Identifying a group in the library

Given an arbitrary group of order at most 2000, can we identify this group in the Small Groups library?

A group whose order has at most 3 prime divisors can be identified following Hölder's analysis of these groups. Hence, for each generic group in the library, we have an effective recognition algorithm available.

By considering its order and testing for normal Hall subgroups, we identify whether a given group is split. If so, we recursively identify its components, R and S, and the operation of S on R.

We now outline two approaches to identify encoded and insoluble groups in the library. The first is a general algorithm to solve the isomorphism problem for p-groups. The second uses invariants of the stored groups.

These methods allow identification of all groups in the library, except those of order 1536.

6.1 Standard presentations for p-groups

O'Brien (1994) presents a practical algorithm to decide isomorphism of two finite p-groups. He defines a *standard presentation* for each p-group and provides an algorithm to construct this presentation. Hence, given two p-groups described by arbitrary presentations, deciding their isomorphism is essentially the same problem as the construction of their standard presentations.

The encoding of a p-group stored in the library is that of the standard presentation of the group. Hence to find the identifier of an arbitrary p-group, we construct its standard presentation, encode this presentation, and locate this encoding in the library.

Implementations of the algorithm are available in GAP and MAGMA.

6.2 Identification via invariants

We computed a list of distinguishing invariants for all encoded groups in the library, except those of orders 512 and 1536. This list of invariants is stored in a compressed format and is 41 MB in size. It provides a very efficient approach to identify an encoded group in the library: we compute certain invariants for the given group and locate them in the stored list.

We use a labelled tree to refine our search. The root node is the set of all groups in the library. Each depth level corresponds to a new invariant; the edges linking children to a parent are labelled by different values of this invariant. Each child node is the subset of groups which take this value for the invariant.

Hence, at each level of the tree, we have a partition of all of the groups and by proceeding downwards, this partition is refined. The leaves usually correspond to single groups; in a few cases they correspond to small sets of groups. (In the latter case we use random isomorphism testing to distinguish among the groups in such a set.) Of course, leaves may be at different levels of the tree.

The invariants at the first two levels of the tree are the group order and the abelian invariants of its derived series. If the group is soluble, we next use invariants of a *special* CGS (Eick, 1997); otherwise we use abelian invariants of its centre. At subsequent levels we consider invariants based on conjugacy classes of elements. We partition the conjugacy classes of a group by element order and class length. We use a 3-tuple to identify each subset of the partition: the number of classes it contains, their representative order, and their length. Then we use power-maps and other mappings related to conjugacy classes to split up the given partition of conjugacy classes. Thus we obtain more refined invariants which we use at subsequent levels.

The algorithm is described in Besche & Eick (1999a, 2000) and an implementation is available in GAP.

Acknowledgements

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. We thank M.F. Newman for helpful comments.

References

Claude Archer (1998), "The extension problem and classification of nonsolvable groups". MSc thesis, Université Libre de Bruxelles.

G. Bagnera (1898), "La composizione dei Gruppi finiti il cui grado é la quinta potenza di un numero primo", *Ann. Mat. Pura Appl. (3)*, **1**, 137–228.

G. Bagnera (1899), "Sopra i gruppi astratti di grado 32", *Ann. Mat. Pura Appl. (3)*, **2**, 263–275.

David Baldwin (1987), "The groups of order 3^n, for $n \leq 6$", BSc thesis. Australian National University.

P.J.H. Baudet (1918), *Groepentheoretische onderzoekingen*, PhD thesis. Groningen University.

H.A. Bender (1927), "A determination of the groups of order p^5", *Ann. of Math.* (2), **29**, 61–72.

Hans Ulrich Besche and Bettina Eick (1999a), "Construction of Finite Groups", *J. Symbolic Comput.*, **27**, 387–404.

Hans Ulrich Besche and Bettina Eick (1999b), "The Groups of Order at Most 1000 Except 512 and 768", *J. Symbolic Comput.*, **27**, 405–413.

Hans Ulrich Besche and Bettina Eick (2000), "The groups of order $q^n \cdot p$", *Comm. Algebra.*

Anton Betten (1996), "Parallel Construction of Finite Solvable Groups", *Parallel Virtual Machine – EuroPVM'96*, Lecture Notes in Comput. Sci., **1156**, (Munich, 1996), pp. 126–133. Springer, Berlin.

N. Blackburn (1958), "On a special class of p-groups", *Acta Math.*, **100**, 45–92.

Wieb Bosma, John Cannon and Catherine Playoust (1997), "The Magma Algebra System I: The User Language", *J. Symbolic Comput.*, **24**, 235–265.

W. Burnside (1897), *Theory of groups of finite order.* Cambridge University Press.

G. Butler, S.S. Iyer and E.A. O'Brien (1993), "TwoGroups: A Database for Group-Theory", *Notices Amer. Math. Soc.*, **40**, 839–841.

A. Cayley (1854), "On the Theory of Groups, as depending on the Symbolic Equation $\theta^n = 1$", *Philos. Mag. (4)*, **7**, 40–47.

A. Cayley (1859), "On the Theory of Groups, as depending on the Symbolic Equation $\theta^n = 1$. - Part III", *Philos. Mag. (4)*, **18**, 34–37.

A. Cayley (1889), "On the theory of groups", *Amer. J. Math*, **11**, 139–157.

F.N. Cole and J.W. Glover (1893), "On groups whose orders are products of three prime factors", *Amer. J. Math.*, **15**, 191–220.

J.-A. de Séguier (1904), *Théorie des groupes finis. Éléments de la théorie des groupes abstraits.* Gauthier-Villars, Paris.

Bettina Eick (1997), "Special Presentations for Finite Soluble Groups and Computing (Pre-)Frattini Subgroups", Amer. Math. Soc. DIMACS Series, **28**, (DIMACS, 1995), pp. 101–112.

Bettina Eick, C.R. Leedham-Green and E.A. O'Brien (2000), "Computing automorphism groups of p-groups", *Preprint.*

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

Wolfgang Gaschütz (1953), "Über die Φ-Untergruppe endlicher Gruppen", *Math. Z.*, **58**, 160–170.

Oliver E. Glenn (1906), "Determination of the abstract groups of order p^2qr; p, q, r being distinct primes", *Trans. Amer. Math. Soc.*, **7**, 137–151.

Marshall Hall, Jr., and James K. Senior (1964), *The Groups of Order* 2^n $(n \leq 6)$. Macmillan, New York.

Charles Hempel (2000), "Metacyclic groups", *Comm. Algebra.*

Graham Higman (1960), "Enumerating p-groups. I: Inequalities", *Proc. London Math. Soc.* (3), **10**, 24–30.

Otto Hölder (1893), "Die Gruppen der Ordnungen p^3, pq^2, pqr, p^4", *Math. Ann.*, **43**, 301–412.

Otto Hölder (1895a), "Bildung zusammengesetzter Gruppen", *Math. Ann.*, **46**, 321–422.

Otto Hölder (1895b), “Die Gruppen mit quadratfreier Ordnungszahl”, *Abh. Akad. Wiss. Göttingen Math.-Phys. Kl.*, 211–229.

Derek F. Holt and W. Plesken (1989), *Perfect Groups.* Clarendon Press, Oxford.

Alexander Hulpke (1996), *Konstruktion transitiver Permutationsgruppen*, PhD thesis. RWTH Aachen.

M.A. Jabber (1941), “Determination of the groups of order 180”, *Bull. Calcutta Math. Soc.*, **33**, 55–70.

Rodney K. James (1968), *The Groups of Order p^6 ($p \geq 3$)*, PhD thesis. University of Sydney.

Rodney James (1980), “The Groups of Order p^6 (p an Odd Prime)”, *Math. Comp.*, **34**, 613–637.

Rodney James, M.F. Newman and E.A. O’Brien (1990), “The Groups of Order 128”, *J. Algebra*, **129**(1), 136–158.

A.B. Kempe (1886), “Memoir on the theory of Mathematical Form”, *Phil. Trans. Roy. Soc. London Ser. A*, **177**, 1–70.

A.M. Küpper (1979), *Enumeration of some two-generator groups of prime power order*, Master’s thesis. Australian National University.

Reinhard Laue (1982), *Zur Konstruktion und Klassifikation endlicher auflösbarer Gruppen*, Bayreuth. Math. Schr., **9**.

R. Levavasseur (1896a), “Sur les groupes d’opérations I”, *C. R. Acad. Sci. Paris Vie Académique*, **122**, 180–182.

R. Levavasseur (1896b), “Sur les groupes d’opérations II”, *C. R. Acad. Sci. Paris Vie Académique*, **122**, 516–517.

R. Le Vavasseur (1899a), “Les groupes d’ordre p^2q^2, p étant un nombre premier plus grand que le nombre premier q”, *C. R. Acad. Sci. Paris Vie Académique*, **128**, 1152–1153.

R. Le Vavasseur (1899b), “Les groupes d’ordre $16p$, p étant un nombre premier impair”, *C. R. Acad. Sci. Paris Vie Académique*, **129**, 26–27.

R. Le Vavasseur (1902), “Les groupes d’ordre p^2q^2, p étant un nombre premier plus grand que le nombre premier q”, *Ann. de l’Éc. Norm. (3)*, **19**, 335–355.

R. Le Vavasseur (1903), “Les groupes d’ordre $16p$, p étant un nombre premier impair”, *Toulouse Ann.*, **5**, 63–123.

Y.K. Leong (1974), "Odd order nilpotent groups of class two with cyclic centre", *J. Austral. Math. Soc. Ser. A*, **17**, 142–153.

Steven Liedahl (1996), "Enumeration of metacyclic p-groups", *J. Algebra*, **186**, 436–446.

Huei-Lung Lin (1974), "On groups of order p^2q, p^2q^2", *Tamkang J. Math.*, **5**, 167–190.

A.C. Lunn and J.K. Senior (1934), "A method of determining all the solvable groups of given order and its application to the orders $16p$ and $32p$", *Amer. J. Math.*, **56**, 319–327.

A.C. Lunn and J.K. Senior (1935), "Determination of the groups of orders 162-215 omitting order 192", *Amer. J. Math.*, **57**, 254–260.

B. Malmrot (1925), *Studien über Gruppen deren Ordnung ein Produkt von sechs Primzahlen ist*, PhD thesis. Uppsala University.

John McKay (1969), "Table errata: *The groups of order* 2^n $(n \leq 6)$ (Macmillan, New York, 1964) by M. Hall, Jr. and J. K. Senior", *Math. Comp.*, **23**, 691–692.

R.J. Miech (1975), "On p-groups with a cyclic commutator subgroup", *J. Austral. Math. Soc. Ser. A*, **20**, 178–198.

G.A. Miller (1896a), "The Operation Groups of order $8p$, p being any prime number", *Philos. Mag. (5)*, **42**, 195–200.

G.A. Miller (1896b), "The regular substitution groups whose orders are less than 48", *Quart. J. Math.*, **28**, 232–284.

G.A. Miller (1898), "On the operation groups whose orders are less than 64 and those whose order is $2p^3$, p being any prime number", *Quart. J. Math.*, **30**, 243–263.

G.A. Miller (1899), "Report on recent progress in the theory of groups of a finite order", *Bull. Amer. Math. Soc.*, **5**, 227–249.

G.A. Miller (1902), "Determination of all the groups of order 168", *Amer. Math. Monthly*, **9**, 1–5.

G.A. Miller (1921a), "An overlooked infinite system of groups of order pq^2", *Proc. Nat. Acad. Sci. USA*, **7**, 146–148.

G.A. Miller (1921b), "An overlooked infinite system of groups of order pq^2, p and q being prime numbers", *Bull. Amer. Math. Soc.*, **27**, 406–407.

G.A. Miller (1929), "Determination of all the Abstract Groups of Order 72", *Amer. J. Math.*, **51**, 491–494.

G.A. Miller (1930a), “Determination of all the Groups of Order 64”, *Amer. J. Math.*, **52**, 617–634.

G.A. Miller (1930b), “Determination of all the groups of order 96”, *Ann. of Math.* (2), **31**, 163–168.

G.A. Miller (1936), “General theorems applying to all the groups of order 32”, *Proc. Nat. Acad. Sci. USA*, **22**, 112–115.

Eugen Netto (1882), *Substitutionentheorie und ihre Anwendungen auf die Algebra.* Teubner, Leipzig.

Joachim Neubüser (1967), “Die Untergruppenverbände der Gruppen der Ordnungen ≤ 100 mit Ausnahme der Ordnungen 64 und 96”. Habilitationsschrift, Kiel.

M.F. Newman (1977), “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.

M.F. Newman and E.A. O’Brien (1986), “Report on the paper - The Groups of Order p^6 (p an Odd Prime)”. Manuscript, Australian National University.

M.F. Newman and E.A. O’Brien (1989), “A CAYLEY library for the groups of order dividing 128”, *Group Theory*, (Singapore, 1987), pp. 437–442. Walter de Gruyter, Berlin, New York.

Ragnar Nyhlén (1919), *Determination of the abstract groups of order $16p^2$ and $8p^3$*, PhD thesis. Uppsala University.

E.A. O’Brien and M.W. Short (1988), “Bibliography on classification of finite groups”. Manuscript, Australian National University.

E.A. O’Brien (1990), “The p-group generation algorithm”, *J. Symbolic Comput.*, **9**, 677–698.

E.A. O’Brien (1991), “The Groups of Order 256”, *J. Algebra*, **143**(1), 219–235.

E.A. O’Brien (1994), “Isomorphism testing for p-groups”, *J. Symbolic Comput.*, **17**, 133–147.

Marie-Martine Patris-Moreau (1975), “Détermination des groupes non résolubles d’ordre inférieur ou égal á 959”, *Acad. Roy. Belg. Bull. Cl. Sci.*, **61**, 658–665.

O.S. Pilyavskaya (1983), “Application of matrix problems to the classification of groups of order p^6, $p > 3$”, *Linear algebra and representation theory*, 86–99.

M. Potron (1904a), *Sur quelques groupes d’ordre p^6*, PhD thesis. Gauthier-Villars, Paris.

M. Potron (1904b), "Sur quelques groupes d'ordre p^6", *Bull. Soc. Math. France*, **32**, 296–300.

László Pyber (1993), "Asymptotic results for permutation groups", Amer. Math. Soc. DIMACS Series, **11**, (DIMACS, 1991), pp. 197–219.

Derek J. Robinson (1996), *A Course in the Theory of Groups* (2nd edition), Graduate Texts in Math., **80**. Springer-Verlag, New York, Heidelberg, Berlin.

Eugene Rodemich (1980), "The Groups of Order 128", *J. Algebra*, **67**, 129–142.

Otto Schreier (1926), "Über die Erweiterung von Gruppen. II", *Abh. Math. Sem. Univ. Hamburg*, **4**, 321–346.

Hyo-Seob Sim (1994), "Metacyclic groups of odd order", *Proc. London Math. Soc.* (3), **69**, 47–71.

Madeleine Sophie (1962), "A note on the groups of order thirty-two", *Illinois J. Math.*, **6**, 630–633.

Derek Roy Taunt (1948), *The theory and method of construction of a particular type of finite solvable group, with special reference to soluble groups of cube-free order*, PhD thesis. Cambridge University.

D.R. Taunt (1955), "Remarks on the isomorphism problem in theories of construction of finite groups", *Proc. Cambridge Philos. Soc.*, **51**, 16–24.

The GAP Team (1997), GAP – *Groups, Algorithms, and Programming, Version* 4. Lehrstuhl D für Mathematik, RWTH Aachen and School of Mathematical and Computational Sciences, University of St Andrews.

Louis William Tordella (1939), *A classification of groups of order p^6, p an odd prime*, PhD thesis. University of Illinois (Urbana).

M.O. Tripp (1909), *Groups of order p^3q^2*, PhD thesis. Columbia University.

Zhi Xiong Wen (1984), "On finite groups of order 2^3pq", *Chinese Ann. Math. Ser. B*, **5**(4), 695–710.

A.E. Western (1899), "Groups of Order p^3q", *Proc. London Math. Soc. (1)*, **30**, 209–263.

David Wilkinson (1988), "The groups of exponent p and order $p \geq 7$ (p any prime)", *J. Algebra*, **118**, 109–119.

J.W.A. Young (1893), "On the determination of groups whose order is a power of a prime", *Amer. J. Math.*, **15**, 124–178.

Yuan Da Zhang (1983), "The structure of groups of order 2^3p^2", *Chinese Ann. Math. Ser. B*, **4**(1), 77–93.

A The number of groups of order at most 2000

	+0	+1	+2	+3	+4	+5	+6	+7	+8	+ 9
0		1	1	1	2	1	2	1	5	2
10	2	1	5	1	2	1	14	1	5	1
20	5	2	2	1	15	2	2	5	4	1
30	4	1	51	1	2	1	14	1	2	2
40	14	1	6	1	4	2	2	1	52	2
50	5	1	5	1	15	2	13	2	2	1
60	13	1	2	4	267	1	4	1	5	1
70	4	1	50	1	2	3	4	1	6	1
80	52	15	2	1	15	1	2	1	12	1
90	10	1	4	2	2	1	231	1	5	2
100	16	1	4	1	14	2	2	1	45	1
110	6	2	43	1	6	1	5	4	2	1
120	47	2	2	1	4	5	16	1	2328	2
130	4	1	10	1	2	5	15	1	4	1
140	11	1	2	1	197	1	2	6	5	1
150	13	1	12	2	4	2	18	1	2	1
160	238	1	55	1	5	2	2	1	57	2
170	4	5	4	1	4	2	42	1	2	1
180	37	1	4	2	12	1	6	1	4	13
190	4	1	1543	1	2	2	12	1	10	1
200	52	2	2	2	12	2	2	2	51	1
210	12	1	5	1	2	1	177	1	2	2
220	15	1	6	1	197	6	2	1	15	1
230	4	2	14	1	16	1	4	2	4	1
240	208	1	5	67	5	2	4	1	12	1
250	15	1	46	2	2	1	56092	1	6	1
260	15	2	2	1	39	1	4	1	4	1
270	30	1	54	5	2	4	10	1	2	4
280	40	1	4	1	4	2	4	1	1045	2
290	4	2	5	1	23	1	14	5	2	1
300	49	2	2	1	42	2	10	1	9	2
310	6	1	61	1	2	4	4	1	4	1
320	1640	1	4	1	176	2	2	2	15	1
330	12	1	4	5	2	1	228	1	5	1
340	15	1	18	5	12	1	2	1	12	1
350	10	14	195	1	4	2	5	2	2	1
360	162	2	2	3	11	1	6	1	42	2
370	4	1	15	1	4	7	12	1	60	1
380	11	2	2	1	20169	2	2	4	5	1
390	12	1	44	1	2	1	30	1	2	5
400	221	1	6	1	5	16	6	1	46	1
410	6	1	4	1	10	1	235	2	4	1
420	41	1	2	2	14	2	4	1	4	2
430	4	1	775	1	4	1	5	1	6	1
440	51	13	4	1	18	1	2	1	1396	1
450	34	1	5	2	2	1	54	1	2	5
460	11	1	12	1	51	4	2	1	55	1
470	4	2	12	1	6	2	11	2	2	1
480	1213	1	2	2	12	1	261	1	14	2
490	10	1	12	1	4	4	42	2	4	1

	+0	+1	+2	+3	+4	+5	+6	+7	+8	+ 9
500	56	1	2	1	202	2	6	6	4	1
510	8	1	10494213	15	2	1	15	1	4	1
520	49	1	10	1	4	6	2	1	170	2
530	4	2	9	1	4	1	12	1	2	2
540	119	1	2	2	246	1	24	1	5	4
550	16	1	39	1	2	2	4	1	16	1
560	180	1	2	1	10	1	2	49	12	1
570	12	1	11	1	4	2	8681	1	5	2
580	15	1	6	1	15	4	2	1	66	1
590	4	1	51	1	30	1	5	2	4	1
600	205	1	6	4	4	7	4	1	195	3
610	6	1	36	1	2	2	35	1	6	1
620	15	5	2	1	260	15	2	2	5	1
630	32	1	12	2	2	1	12	2	4	2
640	21541	1	4	1	9	2	4	1	757	1
650	10	5	4	1	6	2	53	5	4	1
660	40	1	2	2	12	1	18	1	4	2
670	4	1	1280	1	2	17	16	1	4	1
680	53	1	4	1	51	1	15	2	42	2
690	8	1	5	4	2	1	44	1	2	1
700	36	1	62	1	1387	1	2	1	10	1
710	6	4	15	1	12	2	4	1	2	1
720	840	1	5	2	5	2	13	1	40	504
730	4	1	18	1	2	6	195	2	10	1
740	15	5	4	1	54	1	2	2	11	1
750	39	1	42	1	4	2	189	1	2	2
760	39	1	6	1	4	2	2	1	1090235	1
770	12	1	5	1	16	4	15	5	2	1
780	53	1	4	5	172	1	4	1	5	1
790	4	2	137	1	2	1	4	1	24	1
800	1211	2	2	1	15	1	4	1	14	1
810	113	1	16	2	4	1	205	1	2	11
820	20	1	4	1	12	5	4	1	30	1
830	4	2	1630	2	6	1	9	13	2	1
840	186	2	2	1	4	2	10	2	51	2
850	10	1	10	1	4	5	12	1	12	1
860	11	2	2	1	4725	1	2	3	9	1
870	8	1	14	4	4	5	18	1	2	1
880	221	1	68	1	15	1	2	1	61	2
890	4	15	4	1	4	1	19349	2	2	1
900	150	1	4	7	15	2	6	1	4	2
910	8	1	222	1	2	4	5	1	30	1
920	39	2	2	1	34	2	2	4	235	1
930	18	2	5	1	2	2	222	1	4	2
940	11	1	6	1	42	13	4	1	15	1
950	10	1	42	1	10	2	4	1	2	1
960	11394	2	4	2	5	1	12	1	42	2
970	4	1	900	1	2	6	51	1	6	2
980	34	5	2	1	46	1	4	2	11	1
990	30	1	196	2	6	1	10	1	2	15

	+0	+1	+2	+3	+4	+5	+6	+7	+8	+ 9
1000	199	1	4	1	4	2	2	1	954	1
1010	6	2	13	1	23	2	12	2	2	1
1020	37	1	4	2	49487365422	4	66	2	5	19
1030	4	1	54	1	4	2	11	1	4	1
1040	231	1	2	1	36	2	2	2	12	1
1050	40	1	4	51	4	2	1028	1	5	1
1060	15	1	10	1	35	2	4	1	12	1
1070	4	4	42	1	4	2	5	1	10	1
1080	583	2	2	6	4	2	6	1	1681	6
1090	4	1	77	1	2	2	15	1	16	1
1100	51	2	4	1	170	1	4	5	5	1
1110	12	1	12	2	2	1	46	1	4	2
1120	1092	1	8	1	5	14	2	2	39	1
1130	4	2	4	1	254	1	42	2	2	1
1140	41	1	2	5	39	1	4	1	11	1
1150	10	1	157877	1	2	4	16	1	6	1
1160	49	13	4	1	18	1	4	1	53	1
1170	32	1	5	1	2	2	279	1	4	2
1180	11	1	4	3	235	2	2	1	99	1
1190	8	2	14	1	6	1	11	14	2	1
1200	1040	1	2	1	13	2	16	1	12	5
1210	27	1	12	1	2	69	1387	1	16	1
1220	20	2	4	1	164	4	2	2	4	1
1230	12	1	153	2	2	1	15	1	2	2
1240	51	1	30	1	4	1	4	1	1460	1
1250	55	4	5	1	12	2	14	1	4	1
1260	131	1	2	2	42	3	6	1	5	5
1270	4	1	44	1	10	3	11	1	10	1
1280	1116461	5	2	1	10	1	2	4	35	1
1290	12	1	11	1	2	1	3609	1	4	2
1300	50	1	24	1	12	2	2	1	18	1
1310	6	2	244	1	18	1	9	2	2	1
1320	181	1	2	51	4	2	12	1	42	1
1330	8	5	61	1	4	1	12	1	6	1
1340	11	2	4	1	11720	1	2	1	5	1
1350	112	1	52	1	2	2	12	1	4	4
1360	245	1	4	1	9	5	2	1	211	2
1370	4	2	38	1	6	15	195	15	6	2
1380	29	1	2	1	14	1	32	1	4	2
1390	4	1	198	1	4	8	5	1	4	1
1400	153	1	2	1	227	2	4	5	19324	1
1410	8	1	5	4	4	1	39	1	2	2
1420	15	4	16	1	53	6	4	1	40	1
1430	12	5	12	1	4	2	4	1	2	1
1440	5958	1	4	5	12	2	6	1	14	4
1450	10	1	40	1	2	2	179	1	1798	1
1460	15	2	4	1	61	1	2	5	4	1
1470	46	1	1387	1	6	2	36	2	2	1
1480	49	1	24	1	11	10	2	1	222	1
1490	4	3	5	1	10	1	41	2	4	1

	+0	+1	+2	+3	+4	+5	+6	+7	+8	+ 9
1500	174	1	2	2	195	2	4	1	15	1
1510	6	1	889	1	2	2	4	1	12	2
1520	178	13	2	1	15	4	4	1	12	1
1530	20	1	4	5	4	1	408641062	1	2	60
1540	36	1	4	1	15	2	2	1	46	1
1550	16	1	54	1	24	2	5	2	4	1
1560	221	1	4	1	11	1	30	1	928	2
1570	4	1	10	2	2	13	14	1	4	1
1580	11	2	6	1	697	1	4	3	5	1
1590	8	1	12	5	2	2	64	1	4	2
1600	10281	1	10	1	5	1	4	1	54	1
1610	8	2	11	1	4	1	51	6	2	1
1620	477	1	2	2	56	5	6	1	11	5
1630	4	1	1213	1	4	2	5	1	72	1
1640	68	2	2	1	12	1	2	13	42	1
1650	38	1	9	2	2	2	137	1	2	5
1660	11	1	6	1	21507	5	10	1	15	1
1670	4	1	34	2	60	2	4	5	2	1
1680	1005	2	5	2	5	1	4	1	12	1
1690	10	1	30	1	10	1	235	1	6	1
1700	50	309	4	2	39	7	2	1	11	1
1710	36	2	42	2	2	5	40	1	2	2
1720	39	1	12	1	4	3	2	1	47937	1
1730	4	2	5	1	13	1	35	4	4	1
1740	37	1	4	2	51	1	16	1	9	1
1750	30	2	64	1	2	14	4	1	4	1
1760	1285	1	2	1	228	1	2	5	53	1
1770	8	2	4	2	2	4	260	1	6	1
1780	15	1	110	1	12	2	4	1	12	1
1790	4	5	1083553	1	12	1	5	1	4	1
1800	749	1	4	2	11	3	30	1	54	13
1810	6	1	15	2	2	9	12	1	10	1
1820	35	2	2	1	1264	2	4	6	5	1
1830	18	1	14	2	4	1	117	1	2	2
1840	178	1	6	1	5	4	4	1	162	2
1850	10	1	4	1	16	1	1630	2	2	2
1860	56	1	10	15	15	1	4	1	4	2
1870	12	1	1096	1	2	21	9	1	6	1
1880	39	5	2	1	18	1	4	2	195	1
1890	120	1	9	2	2	1	54	1	4	4
1900	36	1	4	1	186	2	2	1	36	1
1910	6	15	12	1	8	1	4	5	4	1
1920	241004	1	5	1	15	4	10	1	15	2
1930	4	1	34	1	2	4	167	1	12	1
1940	15	1	2	1	3973	1	4	1	4	1
1950	40	1	235	11	2	1	15	1	6	1
1960	144	1	18	1	4	2	2	2	203	1
1970	4	15	15	1	12	2	39	1	4	1
1980	120	1	2	2	1388	1	6	1	13	4
1990	4	1	39	1	2	5	4	1	66	1
2000	963									

Hans Ulrich Besche
Lehrstuhl D für Mathematik
RWTH Aachen
Templergraben 64
52062 Aachen
Germany

hbesche@math.rwth-aachen.de

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

eick@mathematik.uni-kassel.de

E.A. O'Brien
Department of Mathematics
University of Auckland
Private Bag 92019
Auckland
New Zealand

obrien@math.auckland.ac.nz

Last revised February 2000