Constructing All Composition Series of a Finite Group

Alexander Hulpke
Department of Mathematics
Colorado State University
1874 Campus Delivery
Fort Collins, CO, 80523-1874, USA
hulpke@math.colostate.edu

ABSTRACT

This paper describes an effective method for enumerating all composition series of a finite group, possibly up to action of a group of automorphisms. By building the series in an ascending way it only requires a very easy case of complement computation and can avoid the need to fuse subspace chains in vector spaces.

As a by-product it also enumerates all subnormal subgroups.

Categories and Subject Descriptors

I.1.2 [**Symbolic and Algebraic Manipulation**]: Algebraic Algorithms

General Terms

Algorithms

Keywords

Finite Groups; Composition series; Subnormal subgroups; Enumeration

1. INTRODUCTION

A composition series, that is a series of subgroups each normal in the previous such that subsequent factor groups are simple, is one of the basic concepts in group theory. The aim of this paper is to describe an effective process for enumerating all composition series of a finite group, possibly up to the action of a group of automorphisms.

While the Jordan-Hölder theorem states that the collection of composition factors (with multiplicity) is an invariant of the group, groups can have a huge number of composition series (see the examples in Section 6.1 below) even when enumerating up to automorphisms. This shows that such an enumeration is a nontrivial task, producing useful information.

ISSAC'15, July 6–9, 2015, Bath, United Kingdom.

DOI: http://dx.doi.org/10.1145/2755996.2756642.

Subgroups that can occur in a composition series are called *subnormal*, thus a list of all subnormal subgroups will be a by-product of such an enumeration.

For solvable groups, the set of all composition series also parameterizes the set of polycyclic presentations, up to a choice of generators of cyclic groups. (A polycyclic presentation [11, Section 8.1] is the standard way of representing solvable groups on a computer.)

A naive approach to enumerating composition series would be to determine the maximal normal subgroups of the whole group and then for each such subgroup U calculate U's maximal normal subgroups in turn, iterating down. If there is a group action one would need to form orbits on each level.

This approach will quickly run into problems. For example consider the group $G = \left(3^5 \rtimes GL_5(3)\right) \times A_5^2$, classifying composition series up to conjugacy in G. For $N = 3^5$ there are 24 partial composition series that descend from G and contain N. The action of $GL_5(3)$ then implies that in each case there is one orbit of composition series through N. The naive approach however would first enumerate maximal subspaces and then fuse them back into one orbit each time, causing much redundancy and making this approach infeasible.

The approach we use instead will only determine the possible composition series in each chief factor once, and then combine these in all possible ways to series for the whole group. Furthermore, the combination step involves calculations that are far easier than the determination of maximal normal subgroups.

2. REDUCTION TO CHIEF FACTORS

We assume globally that G is a finite group, given in a representation that allows us to test membership in subgroups, compute subgroup orders (and their prime number factorizations), as well as compute a chief series for G. This certainly holds for permutation groups and groups given by a PC presentation, which are the cases for which the algorithm has been implemented. Using matrix group recognition [1] there is no fundamental obstacle to apply it also to matrix groups, though implementation would be harder.

This model allows for the test of subgroup membership and computation of subgroup orders in factor groups of G. In that it is nominally stronger than the model of a blackbox group (in which it is only possible to test for element equality) that is sometimes used to describe computations in factor groups; however it models the main classes of representations of finite groups on a computer as used today,

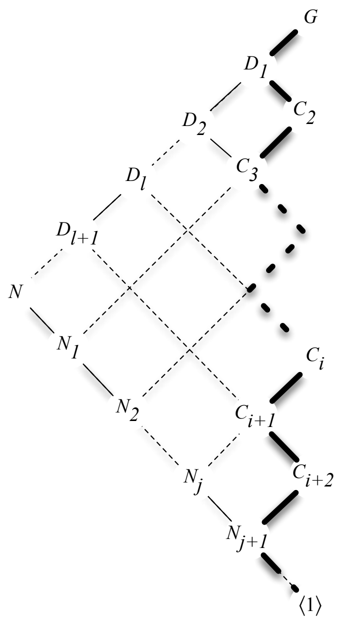

Figure 1: Relation to normal subgroup.

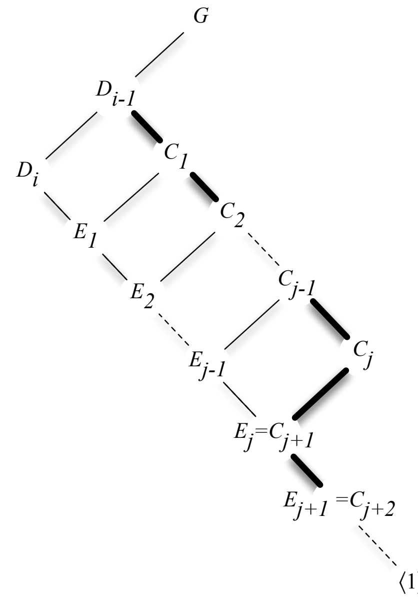

Figure 2: Extension to a single step in the factor group

and avoids technical assumptions (such as the existence of discrete logarithm or element order oracles, or the use of quantum algorithms) that are otherwise sometimes needed in the black-box model.

We identify a series of subgroups $G = C_0 \geq C_1 \geq \cdots \geq C_l = \langle 1 \rangle$ with the set $\{C_i\}$, inclusion providing a natural ordering. (We shall assume that indices are always chosen compatible with inclusion.)

Such a series $\{C_i\}$ is called a *subnormal series* if each subgroup is normal in the previous one, $C_i \lhd C_{i-1}$. It is called a *composition series* if furthermore each factor C_{i-1}/C_i is simple, that is the series is as fine as possible.

If we consider instead the case that all subgroups are normal in G, such a series $\{C_i\}$ is called a *normal series*; if it is maximally refined it is called a *chief series*. In a chief series the subsequent factors C_{i-1}/C_i do not have to be simple, but must be a isomorphic to a direct power of a simple group, that is $C_{i-1}/C_i \cong T_i \times \cdots \times T_i$ with T_i simple. (We say that C_{i-1}/C_i is *characteristically simple*.)

The standard reduction of algorithmic problems in group theory is to consider a normal subgroup $N \lhd G$ and recurse to N and G/N, combining the results in the end.

We now assume that $\{C_i\}$ is a composition series of G and that $N \lhd G$.

A standard exercise in abstract algebra shows that $\{C_i \cap N\}$ forms a composition series for N. (Note that there will be duplication of subgroups, i.e. for some i we have that $C_i \cap N = C_{i+1} \cap N$, though $C_i \neq C_{i+1}$. Considering a series as a set eliminates such duplicates.) Similarly, $\{NC_i/N\}_i$ is a composition series for G/N. As the concatenation of the series NC_i with the series $N \cap C_i$ yields a composition series for G, we easily see that for each i we have that either $NC_i = NC_{i+1}$, or $N \cap C_i = N \cap C_{i+1}$. (See Figure 1)

To see how the enumeration problem reduces, assume that we have classified all composition series for N and for G/N. (The base case of the reduction is that of a characteristically simple group, section 5 describes how to find composition series for these.)

Also assume that we have chosen a particular composition series $N = N_0 \rhd N_1 \rhd \cdots \rhd \langle 1 \rangle$ for N, as well as a particular series of subgroups $G = D_0 \rhd D_i \rhd \cdots \rhd D_k = N$ that induces a composition series for G/N. Our goal now is to determine all composition series $\{C_i\}$ of G such that $\{N \cap C_i\} = \{N_i\}$ and $\{NC_i\} = \{D_i\}$.

We shall construct all these series $\{C_i\}$ in a process of ascending over the series $\{D_i\}$. In each step we assume that the composition series for D_i are known; the base case being the series $\{N_i\}$ for $N = D_k$.

To describe a single step, assume that we have a particular composition series $\{E_j\}$ for D_i and want to find all series $\{C_j\}_j$ for D_{i-1} such that $\{C_j \cap D_i\}_j = \{E_j\}_j$. (Figure 2) As $D_{i-1} \rhd D_i$, the description above shows that there is exactly one step j such that $C_j \cap D_i = C_{j+1} \cap D_i$. We therefore have that $C_{m+1} = E_m$ for $m \geq j$.

For $m \leq j$ we have that $E_m = D_i \cap C_m$ and $C_m = \langle E_m, C_j \rangle$, implying that $E_m \lhd C_m$ and thus $E_m \lhd \langle E_{m-1}, C_m \rangle = C_{m-1}$. Thus in the factor C_{m-1}/E_m, the subgroup C_m/E_m is a normal (as $C_m \lhd C_{m-1}$) complement to E_{m-1}/E_m.

We thus can construct all possible series $\{C_i\}$ in a successive calculation of normal complements, in each step m constructing those series for which $C_m \cap D_i = C_{m+1} \cap D_i$.

We describe this construction in more detail:

Let $C_0 = D_{i-1}$ and take (this will be the series for $j = 0$) the concatenation $C_0 = D_{i-1} \rhd E_0 \rhd E_1 \rhd \cdots \rhd \langle 1 \rangle$. Next, test whether $E_1 \lhd C_0$, if not there are no series for $j > 0$. Otherwise determine all normal complements C_1/E_1 to E_0/E_1 in C_0/E_1. For each such subgroup C_1 we get a series

$C_0 \rhd C_1 \rhd E_1 \rhd \cdots \rhd \langle 1\rangle$; all series for $j = 1$ are obtained this way.

Next, for each of these series, test whether $E_2 \lhd C_1$ and if so determine normal complements C_2/E_2 to E_1/E_2. This yields the series $C_0 \rhd C_1 \rhd C_2 \rhd E_2 \rhd \cdots \rhd \langle 1\rangle$ for $j = 2$.

We continue in the same way for increasing j as long as $E_j \lhd C_{j-1}$, building series that coincide with $\{E_m\}$ for $m \geq j$.

All composition series for D_{i-1} that intersect with D_i in $\{E_j\}$ are obtained this way, iterating over all series for D_i thus yields all composition series for D_{i-1}.

The only task required for combining these series is the construction of normal complements in a factor group that has composition length two. We describe how to do this in section 3.

If we want to determine composition series only up to the action of some group $\leq \mathrm{Aut}(G)$ a further fusion becomes necessary. We shall describe how to do this in section 4.

3. NORMAL COMPLEMENTS

In this section we describe the required computation of normal complements. While this can be done by cohomological methods from [7], these become overly costly given the frequency of calculations required. Instead we shall describe direct methods for the required case of factor groups of composition length two.

For ease of description we denote this factor group by H and the normal subgroup to be complemented by $A \lhd H$ though in practice both are factors of subgroups of G and as described in [14] we work with representatives of elements and pre-images of subgroups.

Theorem 1. *Let H be a finite group and $A \lhd H$ such that A and H/A are both nontrivial simple groups. Then normal complements to A in H are given by the following classification:*

a) If A is not abelian there is at most one complement, namely $C_H(A)$ if this group is nontrivial. If H/A also is not abelian, such a complement always exists.

b) If A is abelian but H/A not, there is at most one complement, namely H', this group is a complement if and only if $H' \neq H$.

(The remaining two cases now assume that both A and H/A are abelian, that is cyclic of prime order.)

c) If $|A| \neq |H/A|$ there is exactly one complement and this is the case if and only if $[H, A] = \langle 1\rangle$.

d) Otherwise there are either 0, or q, normal complements (where $q = |A|$). The case of no complements occurring exactly when $|x| = q^2$ for one (and thus for all) $x \notin A$.

Proof. The existence of a normal complement B is equivalent to $H = A \times B$ (with $B \cong H/A$).

a) If A is not abelian we have that $C_H(A) \cap A = \langle 1\rangle$. If $C_H(A)$ is not trivial it thus is a complement (since $A \neq AC_H(A) \lhd H$ and H/A is simple). Vice versa, if a normal complement B exists, we must have that $B = C_H(A)$. By the proof of Schreier's conjecture (see [9]) the outer automorphism group $\mathrm{Out}(A)$ is solvable for a simple nonabelian A. Thus if H/A is nonsolvable, every element of H must induce an inner automorphism which shows that in this case $C_H(A)$ is not trivial.

In all other cases A is abelian, $|A| = q$ prime, and thus it is a necessary condition for the existence of a normal complement that $A \leq Z(H)$.

b) If H/A is simple nonabelian, then $AH' = H$. Thus if $H' \neq H$ we must have that $A \cap H' = \langle 1\rangle$ and H' is a normal complement to A. Vice versa if $B \cong H/A$ is a normal complement we have that $H' = (A \times B)' = B' = B$.

In the remaining cases we have that both A and H/A are abelian. Thus a necessary condition for the existence of normal complements is that $A \leq Z(H)$, that is $[H, A] = \langle 1\rangle$. But then $H/Z(H)$ is cyclic and thus H is abelian. We shall assume this now.

c) If $|A| \neq |H/A|$ the complements to A are simply p-Sylow subgroups for $p = |H/A|$. As H is abelian there is only one such subgroup.

d) Otherwise $|H| = q^2$ for q prime. If $H \cong C_{q^2}$ there is no complement, if $H \cong C_q \times C_q$ there are q complements, all normal. □

We give more details on how to find these complements in practice:

3.1 Nonabelian normal subgroup

In this section we assume that A is simple nonabelian. We may assume that we know the isomorphism type of A, for example from recognition performed when setting up the initial data structure for G, following [3, 16].

Assume initially that H is a direct product. Our task is to find a nontrivial element $c \in C_H(A)$. (One such element is sufficient, as $C_H(A) \cong H/A$ is assumed to be simple and thus minimally normal. Therefore $C_H(A) = \langle c\rangle_H$ will be the normal closure in H of $\langle c\rangle$.)

The basic process of decomposing a group into direct factors in a black-box context is already described in [2]. As we do not know whether the group is a direct product we describe a variant that also can prove the non-existence of a direct product decomposition. (Note that in some cases we know a priori that H must be a direct product, for example if $[H{:}A]$ is not prime, or if it does not divide $|\mathrm{Out}(A)|$.)

To find centralizing elements we set up the following probabilistic process: Choose one $x \in H$, $x \notin A$. By taking a suitable power of x we may assume without loss of generality that $x^p \in A$ for a prime $p| \, [H{:}A]$.

Now repeatedly choose (pseudo-)random elements $r \in A$ (using for example [6]) and test whether $|rx| = pq$ with $\gcd(p, q) = 1$. In this case, form $c = (rx)^q$ and test whether the nontrivial element c centralizes A. If so, it is a centralizing element as desired.

To see that this process is likely to succeed, write $x = (a, b)$ with $a \in A$, $b \in C_H(A)$. We know that $|b| = |Ax| = p$. If $r \in A$ is chosen randomly, then $rx = (ra, b)$ with ra ranging randomly over A.

But by [4] there is a fair probability w that a random element of A is of order coprime to p. (Concretely, [4] prove that $w \geq 2/29$ for a sporadic A; $w \geq 26/(27\sqrt{n})$ for $A \cong A_n$; $w \geq 1/(2n)$ if A is classical with a natural projective action in dimension $n - 1$; and $w \geq 1/15$ for sporadic A.)

Thus with probability w we have that $|ra| = q$ is coprime to p. In this case $|rx| = pq$ with $\gcd(p, q) = 1$ and

$c = (rx)^q = \big((ra)^q, b^b\big) = (1, b^q)$ is a nontrivial element of $C_H(A)$.

If $C_G(H)$ is not trivial, this test will succeed with probability $1-(1-w)^k$ after k iterations.

If this test fails, however, we need to prove that A has no normal complement in H. We may assume here that $[H{:}A] = p$ is prime, as otherwise the existence of a normal complement is guaranteed. What we have to show is that $H \cong A.C_p \leq \mathrm{Aut}(A)$.

Generically, this amounts to recognizing the structure of H: For example one could consider the conjugation action of H on A, and use black-box recognition to test whether the group is isomorphic to A. In practice one often can do much better:

The process of searching for a centralizing element described above produces elements rx that are chosen randomly over one coset of A. As we assume that H/A is of prime order, the orders of rx thus sample the element orders of H outside A.

If $|rx|$ is an order that does not arise in A, and the power $(rx)^q$ used above does not centralize A we can deduce that H is not a direct product. This is because $(a,b) \in A \times C_p$ has element order $|(a,b)| = \mathrm{lcm}(|a|, |b|)$. This differs from the order of a only if $|b| = p$ is coprime to $|a|$, but this is exactly the case in which the order-p power is $(1,b)$ and centralizes A.

An inspection of nonabelian simple groups up to order $2 \cdot 10^{13}$ (i.e. groups smaller than $G_2(9)$) reveals that (excluding groups of the form $\mathrm{L}_2(q)$ which always have such elements) 104 of the 117 simple groups A have such elements in every extension in $\mathrm{Aut}(A)$, all with ratio at least 1/200. The only exceptions are (all for $p = 2$): $U_3(3)$, $L_3(5)$, $U_3(7)$, $S_4(8)$, $L_3(17)$, $U_3(19)$, $U_5(3)$, $L_3(29)$, $U_3(31)$, $L_3(41)$, $O_8^-(3)$, and $PSU(3,43)$.

Even if element orders do not allow to recognize the case of not being a direct product, the group H arises in our situation not on its own, but as a subfactor of the larger group G. As part of the initial setup (section 6) we might have set up already (e.g. as in [12]) an epimorphism from G onto $G/\mathrm{Rad}(G)$ with the image that lies in (a direct product) of groups of type $\mathrm{Aut}(T) \wr S_m$ for T simple nonabelian. Then H is not to be a direct product if and only if the image of H under this homomorphism has order $|A| \cdot p$ and does not lie in the subgroup $T \wr S_m$. This is readily tested.

3.2 Abelian normal subgroup

If $A \cong C_p$ is abelian and H/A is simple nonabelian then A must be central, as H/A has no nontrivial representation in dimension 1. The two possible extensions thus are either the direct product, or (a quotient of) a covering group of H/A. The latter can only happen if $|A|$ divides the multiplier order $|M(H/A)|$. (Again we may assume we know the isomorphism type of H/A, thus we know this multiplier order.)

By theorem 1, we know that $H = A \times H'$ if it is a direct product. To find this decomposition (and test the condition) we form one nontrivial random commutator c and let $C = \langle c \rangle_H \leq H'$ be the normal closure of this commutator. If $A \leq C$ then no normal complement to A exists (as every commutator would have trivial A-part and thus lie in such a complement). Otherwise $C \lhd H$ with $AC = H$ and $A \cap C = \langle 1 \rangle$, thus it is a normal complement.

To avoid calculating normal closures unnecessarily, we observe that many cases of not being a direct product can be deduced by element orders alone:

Definition 2. Let $A \leq Z(H)$. We call $x \in H$ *order-increasing* if $|Ax|$ is a multiple of $|A|$ and $|x| \neq |Ax|$.

Many covers of simple groups contain such elements, for example in $\mathrm{SL}_2(p)$ (cover of $\mathrm{PSL}_2(p)$) the element $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ is order-increasing.

LEMMA 3. *If $H = A \times B$ then H contains no order-increasing element.*

PROOF. Assume that if $x = (a,b) \in H$ fulfills that $|Ax| = |b|$ is a multiple of $|A|$. Then $|x| = |Ax|$, since $x^{|Ax|} = x^{|b|} = (a^{|b|}, b^{|b|}) = 1$, as by assumption $|b|$ is a multiple of $|a|$). □

We thus initially test the generators of H (and a couple of random elements) whether they are order-increasing. If such an element is found, H cannot be a direct product, and we do not need to calculate a normal closure of a commutator.

If both A and H/A are abelian but $|A| \neq [H{:}A]$ we first test that A is central in H (if not, H is not a direct product). If so, we obtain a complement by choosing $x \in H$, $x \notin A$ and forming $C = \langle x^{|A|} \rangle$.

Finally, if A and H/A are abelian and $|A| = [H{:}A]$ we take $x \in H$, $x \notin A$. If $|x| = p = |A|$ we have that H is a vector space with basis $\{x, a\}$ (where $A = \langle a \rangle$), The elements $x \cdot a^k$, $0 \leq k < p$ then are generators for the normal complements.

If on the other hand $|x| \neq p$, then $H \cong C_{p^2}$ is not a direct product.

3.3 Cost

The required computations for finding all normal complements are (in a Las Vegas model, i.e the calculation might fail with bounded probability, in which case it can be repeated with new random selections) one of the following:

- A constant number of element order computations in a factor group.
- Computation of a derived subgroup.
- Constructive recognition of black-box simple groups (in the fall-back case for identifying outer automorphism actions).

The first two are known to be polynomial time in the size of the input. The third is (possibly Monte-Carlo, possibly assuming a discrete logarithm oracle) polynomial time for most classes of simple groups groups [8, 15, 13], with the exception of composition factors of type ${}^2G_2(q)$. One can of course dispense with these qualifiers if the size of nonabelian composition factors is bounded.

4. ACTION ON SERIES

If we want to construct series only up to the action of a group A (for example the full, or the inner automorphism group) we associate with every (partial) series a stabilizer (namely the intersection of the A-normalizers of the subgroups in the series). We also replace chief factors by A-invariant normal factors. These still must be characteristically simple.

If the normal subgroup $N \lhd G$ is chosen to be invariant under A, then the stabilizer of a subgroup X also stabilizes NX and $N \cap X$, thus in the above construction process we may assume that the acting group is stabilizing the series $\{N_i\}$ in N and $\{D_i\}$ in the factor group. The construction process described above is thus compatible with maintaining series stabilizers.

Now consider the effect of a group action on the combination process. Its basic step is that, for a given j, we have a series (figure 2) $D_{i-1}, C_1, C_2, \ldots, C_j, E_j = C_{j+1}, E_{j+1}, \ldots$, with an associated stabilizer S, and we are looking for series that differ in the group E_j by classifying (normal) complements to E_j/E_{j+1} in C_j/E_{j+1}. The series stabilizer S will act on these complements. (In cases a,b,c) of Theorem 1 there is at most one complement, which automatically is stabilized if it exists. In case d) the action is a projective action on the vector space C_j/E_{j+1}.)

Representatives of the S-orbits then correspond to A-classes of series that arose from the prior series, with complement stabilizers becoming stabilizers for the new series.

5. ELEMENTARY FACTORS

To utilize the reduction of Section 2 we need to obtain the composition series of the chief factors of G (or, in the case of an A-action, A-invariant normal factors, up to A action). Such factors are characteristically simple, i.e. they are direct powers of simple groups of one isomorphism type.

Again for ease of description we describe the construction in a factor group, that is we consider $H \cong T \times \cdots \times T$ for T simple, possibly with a (possibly trivial) action of a group A on H.

5.1 Abelian Case

If T (and thus H) is abelian, a composition series for H is equivalent to a flag, i.e. a sequence of increasing subspaces of dimensions $1, 2, 3 \ldots$. We construct these flags in increasing dimension: First determine the A-orbits on 1-dimensional subspaces of H. For each such subspace U we consider recursively the factor space H/U with action of $S = \mathrm{Stab}_A(U)$ and determine S-representatives of the flags on H/U. For each such flag $U_2/U, U_3/U, \ldots$ for H/U we have that $U, U_2, U_3, \ldots$ is a flag for H. Collecting these flags for all representatives U produces representatives of the A-orbits on flags and thus of the A-orbits of composition series.

5.2 Nonabelian Case

If T is nonabelian then the only normal subgroups of $H = T^m$ are the obvious direct products of subsets of the copies of T. Applying the same statement to these normal subgroups we find that any subnormal subgroup of H must be one of these normal subgroups. Thus the composition series of H are parameterized (indicating in each step which direct factor is added to the subgroup) by the permutations of $\{1, \ldots, m\}$.

The action of A permutes the m direct factors, and thus their indices. Let $\varphi\colon A \to S_m$ be the corresponding homomorphism. On permutations, representing subnormal series, this action is by right multiplication by A^φ. Representatives of the orbits are obtained as representatives for the left cosets of A^φ in S_m, in each case the stabilizer of the series is the kernel of φ.

6. COMBINING THE STEPS

Assume that a group G as well as a group $A \le \mathrm{Aut}(G)$ are given. To describe the A-orbits on composition series for G we adapt the standard "Trivial-Fitting" (or "Solvable Radical") method [2, 5]: Consider the series $G \rhd Pker \rhd S^* \rhd R\langle 1\rangle$ of characteristic subgroups, where R is the solvable radical (the largest solvable normal subgroup), $S^*/R = \mathrm{Soc}(G/R)$ and $Pker$ is the kernel of the permutation action of G on the direct factors of S^*/R. We refine this series to a series of A-invariant normal subgroups $G = N_0 > N_1 > \cdots > N_{k-1} > N_k = \langle 1\rangle$ with N_i/N_{i+1} elementary. As most calculations involving the action of A happen in elementary abelian factors, and as the composition process itself extends *up*, it seems to be most plausible to work *ascending* along this series with decreasing k, starting with $N_{k-1}/\langle 1\rangle$.

In each step we assume we have all A-classes of composition series of N_i. For each such class we have a representative and a series stabilizer.

For each different N_i-series stabilizer S, we determine the S-classes of series through the elementary factor N_{i-1}/N_i. We then use the process from section 2 to form all combinations of these series with those N_i-series for which S is the stabilizer.

As the examples below show, the number of composition series can be easily exponential (or worse) in the size of the input. The algorithm therefore cannot be in polynomial time. However each new series is the result of one complement computation, and the total number of complement computations (including those that do not lead to new series) for each series is the number of composition steps. Since each complement calculation is (with qualifiers as given in section 3.3) polynomial time, the algorithm is therefore overall of polynomial delay.

6.1 Implementation and Examples

The algorithm has been implemented by the author in the system GAP [10].

Table 1 gives examples of calculations of series. Series were calculated under the action of the group itself (column **G-Orbits**), respectively under the full automorphism group (column **Aut(G)**). Timings are in seconds on a 3.7 GHz Quad-Core Intel Xeon E5 Mac Pro (Late 2013). Groups were represented by a PC presentation or as permutation group. Names $\mathrm{t}_d\mathrm{n}_x$ or $\mathrm{s}_d\mathrm{n}_x$ are from the transitive, respectively the small groups library. Using the indices of the stabilizers in the acting group, the total number of series **NrSeries** was computed. An arrow $\to$ indicates that the automorphism group provides no further fusion.

One notes that runtime is roughly proportional to the number of composition series representatives (which is as good as one might hope for). Calculations under the automorphism group take longer for the need to work with stabilizers that were represented as groups of automorphisms.

Group	Order	NrSeries	G-Orbits	time	Aut(G)-Orb.	time
$t_{30}n_{3000}$	$2^{10}3^4 5^3$	318	53	0.5	49	3.2
$3^5 \rtimes GL_5(3)$	$2^{10}3^{15}5{\cdot}11^2 13$	503360	2	1.3	→	
$3^5 \rtimes GL_5(3) \times A_5^2$	$2^{14}3^{17}5^3 11^2 13$	36241920	144	54	72	50
$3^6 \rtimes SP_6(3)$	$2^{10}3^{15}5{\cdot}7{\cdot}13$	91611520	15	6.5	→	
Weyl(F_4)	$2^7 3^2$	13482	377	0.25	204	0.5
$s_{1152}n_{157000}$	$2^7 3^2$	116802	24998	13.5	12000	17
$2^{4+1+1} \rtimes A_5$	$2^8 3{\cdot}5$	645435	12339	41	2214	15
$(3^5.2) : S_5 = t_{30}n_{1254}$	$2^4 3^6 5$	1015040	13296	34	7816	34
$GL_2(5) \wr S_2$	$2^{11}3^2 5^2$	2314	928	4	794	9
$SL_2(5) \wr D_8$	$2^{15}3^4 5^4$	143160	17895	96	17641	504
$GU_3(3) \wr S_2$	$2^{15}3^6 7^2$	890	388	7	257	75
$PGU_3(3) \wr D_8$	$2^{23}3^{12}7^4$	200	25	3.6	→	
$s_{256}n_{100}$	2^8	22287	4124	3.5	3451	11
$s_{256}n_{6000}$	2^8	90651	17763	16	10042	37
$s_{256}n_{10000}$	2^8	429219	212661	226	94964	478
$s_{256}n_{20000}$	2^8	124875	57017	50	49749	147
$s_{256}n_{56000}$	2^8	14252283	5345253	42433[a]	621047	3216

[a] identifying duplicate subgroups, at extra cost, for memory reasons.

Table 1: Examples and Runtimes

7. ACKNOWLEDGMENTS

The author is would like to thank Hoon Hong for suggesting the problem.

The author's work has been supported in part by Simons Foundation Collaboration Grant 244502 which is gratefully acknowledged.

8. REFERENCES

[1] H. Bäärnhielm, D. Holt, C. R. Leedham-Green, and E. A. O'Brien. A practical model for computation with matrix groups. *J. Symbolic Comput.*, 68(part 1):27–60, 2015.

[2] L. Babai and R. Beals. A polynomial-time theory of black box groups. I. In C. M. Campbell, E. F. Robertson, N. Ruskuc, and G. C. Smith, editors, *Groups St Andrews 1997 in Bath*, volume 260/261 of *London Mathematical Society Lecture Note Series*, pages 30–64. Cambridge University Press, 1999.

[3] L. Babai, W. M. Kantor, P. P. Pálfy, and Á. Seress. Black-box recognition of finite simple groups of Lie type by statistics of element orders. *J. Group Theory*, 5(4):383–401, 2002.

[4] L. Babai, P. P. Pálfy, and J. Saxl. On the number of p-regular elements in finite simple groups. *LMS J. Comput. Math.*, 12:82–119, 2009.

[5] J. Cannon, B. Cox, and D. Holt. Computing the subgroup lattice of a permutation group. *J. Symbolic Comput.*, 31(1/2):149–161, 2001.

[6] F. Celler, C. R. Leedham-Green, S. H. Murray, A. C. Niemeyer, and E. A. O'Brien. Generating random elements of a finite group. *Comm. Algebra*, 23(13):4931–4948, 1995.

[7] F. Celler, J. Neubüser, and C. R. B. Wright. Some remarks on the computation of complements and normalizers in soluble groups. *Acta Appl. Math.*, 21:57–76, 1990.

[8] H. Dietrich, C. R. Leedham-Green, and E. A. O'Brien. Effective black-box constructive recognition of classical groups. *J. Algebra*, 421:460–492, 2015.

[9] W. Feit. Some consequences of the classification of finite simple groups. In *The Santa Cruz Conference on Finite Groups (Univ. California, Santa Cruz, Calif., 1979)*, volume 37 of *Proc. Sympos. Pure Math.*, pages 175–181. Amer. Math. Soc., Providence, R.I., 1980.

[10] The GAP Group, `http://www.gap-system.org`. *GAP – Groups, Algorithms, and Programming, Version 4.7.4*, 2014.

[11] D. F. Holt, B. Eick, and E. A. O'Brien. *Handbook of Computational Group Theory*. Discrete Mathematics and its Applications. Chapman & Hall/CRC, Boca Raton, FL, 2005.

[12] A. Hulpke. Computing conjugacy classes of elements in matrix groups. *J. Algebra*, 387:268–286, 2013.

[13] S. Jambor, M. Leuner, A. C. Niemeyer, and W. Plesken. Fast recognition of alternating groups of unknown degree. *J. Algebra*, 392:315–335, 2013.

[14] W. M. Kantor and E. M. Luks. Computing in quotient groups. In *Proceedings of the* 22nd *ACM Symposium on Theory of Computing, Baltimore*, pages 524–563. ACM Press, 1990.

[15] W. M. Kantor and K. Magaard. Black box exceptional groups of Lie type II. *J. Algebra*, 421:524–540, 2015.

[16] M. W. Liebeck and E. A. O'Brien. Finding the characteristic of a group of Lie type. *J. London Math. Soc. (2)*, 75(3):741–754, 2007.