# Calculation of the Subgroups of a Trivial-Fitting Group

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

## ABSTRACT

We describe an algorithm to determine representatives of the conjugacy classes of subgroups of a Trivial-Fitting group, this case being the one prior algorithms reduce to. As a subtask we describe an algorithm for determining conjugacy classes of complements to an arbitrary normal subgroup if the factor group is solvable.

## Categories and Subject Descriptors

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

## Keywords

Subgroups; Complement; Trivial-Fitting; Permutation group; Matrix group

## 1. INTRODUCTION

The question for determining the subgroups of a finite group is one of the earliest [Neu60] problems considered by computational group theory. It also is the task most frequently requested by users [Can11] which gives it extra prominence.

To save on memory this task is usually performed up to conjugacy in the group, that is the equivalence relation $U \sim U^g = g^{-1}Ug$ for $g \in G$. One thus determines for each such class (called a conjugacy class) a representative $U$, as well as its normalizer $N_G(U)$. A basic result about group actions then states that the elements of this class are in bijection with the cosets of $N_G(U)$ in $G$, in particular there are exactly $[G : N_G(U)]$ subgroups in the conjugacy class.

The method currently in use [CCH01] for determining the classes of subgroups uses the Trivial-Fitting paradigm: Let $R \lhd G$ be the largest solvable normal subgroup. First determine the classes of subgroups of $G/R$, then lift the result to $G$ by complement computations. We shall concentrate on this first step, the subgroups of $H = G/R$. This group has no solvable normal subgroups and is thus called a Trivial-Fitting group.

The methods that have been suggested for determining the subgroups of $H$ have been the use of pretabulated data, reduction to maximal subgroups, or the older method of cyclic extension; all of which are rather limited in scope. Instead we will describe a construction that uses the particular structure of such Trivial-Fitting groups as a subgroup of a direct product of wreath products. Section 2 summarizes this structure. Our construction has similarities with the enumeration of transitive subgroups of symmetric groups [Hul05], though of course here we do not impose any limiting conditions on the subgroups and face a more general situation. (In particular complements will arise for normal subgroups that are not solvable, see section 5.) The process also can be taken as a model for the problem of describing subgroups of a wreath product, a problem which sometimes arises in a combinatorial context.

Indeed the work in this paper has been motivated by the question of determining Möbius numbers for symmetric groups [Mon12, Sha97]; for settling the still open case of $S_{18}$ a list of subgroups of $S_6 \wr S_3$ were desired.

## 2. TRIVIAL-FITTING GROUPS

Let $H$ be a finite group with no solvable normal subgroup. Then the following well-known [BB99] facts hold:

Let $S = \mathrm{Soc}(H) \lhd H$ be the *socle* of $H$, that is the normal subgroup generated by all minimal normal subgroups. Then $S$ is the direct product of simple nonabelian groups and $H$ acts faithfully by conjugation on $S$, thus we can consider $H$ as a subgroup of $\mathrm{Aut}(S)$. If the direct factors of $S$ are the simple groups $T_i$ $(i = 1, \ldots, k)$, each arising with multiplicity $n_i$ (that is $S = \bigtimes_i \bigtimes_{j=1}^{n_i} T_i$), then

$$\mathrm{Aut}(S) = \mathrm{Aut}(T_1) \wr S_{n_1} \times \cdots \times \mathrm{Aut}(T_k) \wr S_{n_k}$$

where $\wr$ denotes a permutational wreath product (that is $A \wr S_n = (\underbrace{A \times \cdots \times A}_{n \text{ copies}}) \rtimes S_n$ with $S_n$ acting by permuting the copies of $A$. We shall assume that we have $H$ represented as a subgroup of $\mathrm{Aut}(S)$ and thus can decompose according to this product structure. We then can embed

$$H/S \leq (\mathrm{Aut}(T_1)/T_1) \wr S_{n_1} \times \cdots \times (\mathrm{Aut}(T_k)/T_k) \wr S_{n_k}.$$

By the proof of Schreier's conjecture [Fei80], each $\mathrm{Aut}(T_i)/T_i$ is solvable and comparatively small. (If $T_i$ is of Lie type defined over $\mathbb{F}$, then $\mathrm{Aut}(T_i)/T_i \leq \mathbb{F}^* \rtimes \mathrm{Gal}(\mathbb{F}/\mathbb{F}_p) \rtimes C_2$;


*ISSAC'13,* June 26–29, 2013, Boston, Massachusetts, USA.

otherwise $|\mathrm{Aut}(T_i)/T_i| \leq 4$.) Thus if $a$ is a bound for all $\big[\mathrm{Aut}(T_i){:}T_i\big]$, and we set $n = \sum n_i$ we have that

$$[H{:}S] \leq a^n \cdot n! \tag{1}$$

In practice $n$ has to be comparatively small (it is unlikely that $n$ will be substantially larger than 5 as the total number of subgroup classes otherwise becomes infeasibly large for storage purposes), thus in practice this index $[H{:}S]$ will rarely be larger than a few 10000.

We thus see that $S$ constitutes a large part of $H$ and we shall use this fact in our construction: We first determine the conjugacy classes of subgroups of $S$, then fuse these to $H$-classes of subgroups of $S$ and finally extend to classes of subgroups of $H$.

The structure of $H$ as a subdirect product also means that it is feasible to represent it as a permutation group [Hular, Section 3]. In such a representation, we can determine subgroup normalizers, and test for subgroup conjugacy (constructively, that is finding a conjugating element) using standard backtrack methods [Hol91, Leo97, The97], [HEO05, Section 4.6].

## 3. SUBDIRECT PRODUCTS

The first step is to determine $S$-classes of subgroups of $S$. As $S$ is a direct product of simple groups this is straightforward, using the concept of a subdirect product [Rem30]. Their computational construction is well understood (for example see [HP89] for an earlier application) and a description of how to enumerate their subgroups is found in [Hol10]. The content of this section thus is included only to make this paper self-contained. The section can easily be skipped by an experienced reader.

For simplicity we shall describe the case of a direct product of two factors. The case of multiple factors follows by induction by treating a product $F \times G \times H$ as $(F \times G) \times H$.

Consider a direct product $S = G \times H$. Then $S$ has two projections $\alpha\colon S \to G$ and $\beta\colon S \to H$. A subgroup $U \leq S$ then yields two images $A = U^\alpha \leq G$ and $B = U^\beta \leq H$. If we want to classify subgroups of $S$ up to $S$-conjugacy, we clearly can assume that $A$ is chosen up to $G$-conjugacy and $B$ chosen up to $H$-conjugacy, conjugacy thus is reduced to $N_G(A) \times N_H(B)$.

To describe $U$ further, consider the elements of $U$ that project trivially on one of the components. Thus let $D = (\ker \beta_U)^\alpha \lhd A$ and $E = (\ker \alpha_U)^\beta \lhd B$ (where $\alpha_U$ means the restriction of $\alpha$ to $U$). If we denote the natural homomorphisms by $\rho\colon A \to A/D$ and $\sigma\colon B \to B/E$ then every element of $A/D$ can be written as $(u^\alpha)^\rho$ for a suitable $u \in U$, similarly $\beta\sigma$ maps from $U$ onto $B/E$. We thus can define a map $\zeta\colon A/D \to B/E$ by $(u^\alpha)^\rho \mapsto (u^\beta)^\sigma$. As $\ker\alpha \cap \ker\beta = \langle 1\rangle$ this is well defined. It is easily seen that $\zeta$ is an isomorphism.

Clearly conjugates of $D$ and $E$ under $N_G(A)$ and $N_G(B)$ will lead to conjugates of $U$. When fixing $D$ and $E$ we thus can restrict conjugacy to $N \times M$ where $N = N_{N_G(A)}(D) = N_G(A) \cap N_G(D)$ and $M = N_{N_G(B)}(E) = N_G(B) \cap N_G(E)$.

The set of isomorphisms $A/D \to B/E$ is parameterized by $\mathrm{Aut}(A/D) \cong \mathrm{Aut}(B/E)$. Conjugation by $N$ induces a subgroup $I_N \leq \mathrm{Aut}(A/D)$, conjugation by $M$ one of $\mathrm{Aut}(B/E)$. If we fix one isomorphism $\zeta_0\colon A/D$ (and also denote the induced isomorphism $\mathrm{Aut}(A/D) \to \mathrm{Aut}(B/E)$ by $\zeta_0$), then conjugacy by $N \times M$ corresponds to a double coset in $I_N \setminus \mathrm{Aut}(A/D)/(I_M)^{\zeta_0^{-1}}$.

We have thus seen the following parameterization of $S$-classes of subgroups of the direct product $S$:

THEOREM 1. *[Hul96, Satz 32] For two finite group $G, H$ let $\mathcal{A}$ be a set of representatives of the conjugacy classes of subgroups of $G$ and $\mathcal{B}$ be a set of representatives of the conjugacy classes of $H$. Then a set of representatives of the conjugacy classes of subgroups of $G \times H$ is obtained in the following way:*

- *For each pair $A \in \mathcal{A}$, $B \in \mathcal{B}$ let $\mathcal{D}$ be a set of representatives of the $N_G(A)$-conjugacy classes of normal subgroups of $A$, $\mathcal{E}$ be a set of representatives of the $N_H(B)$-conjugacy classes of normal subgroups of $B$.*
- *For each pair $D \in \mathcal{D}$, $E \in \mathcal{E}$ (with natural homomorphisms $\rho\colon A \to A/D$, $\sigma\colon B \to B/E$) such that there is an isomorphism $\zeta_0\colon A/D \to B/E$ let $N = N_{N_G(A)}(D)$ and $M = N_{N_G(B)}(E)$. Let $\mathcal{Z}$ be a set of representatives of the double cosets $I_N \setminus Aut(A/D)/(I_M)^{\zeta_0^{-1}}$, where $I_N$ are the automorphisms of $A/D$ induced by conjugation with $N$, $I_M$ the automorphisms of $B/E$ induced by $M$.*
- *For each $\zeta \in \mathcal{Z}$ form the subgroup*

$$U := \Big\{(a,b) \in G \times H \mid a \in A, b \in B, (a^\rho)^\zeta = b^\sigma\Big\}$$

*These subgroups $U$ form representatives of the $S$-conjugacy classes of subgroups. The normalizer of $U$ is the subgroup of $N \times M$ which stabilizes $\zeta$ via the induced action of $I_N$ and $I_M$.*

PROOF. The argument before the theorem statement yields the parameterization of subgroups. For such a subgroup $U$ to be normalized, clearly the projections $A$ and $B$, as well as the kernels $E$ and $F$, must be stabilized by conjugation, so $N_S(U) \leq N \times M$. If the isomorphism $\zeta$ defining $U$ is stabilized by an element $x \in N \times M$ then $U^x \subset U$, and otherwise not, thus the stabilizer of $\zeta$ is exactly the normalizer of $U$. □

Note that this parameterization leads in an obvious way to an algorithm to enumerate representatives of the classes of subgroups of $G \times H$ and their normalizers. (We represent $\mathrm{Aut}(A/D)$ as permutation group to determine double cosets.) To find possibly pairings for isomorphic factor groups it can be useful to identify the isomorphism type of small factor groups first, using invariants obtained from the explicit list [BEO02].

We run this algorithm iteratively for a direct product of more than two factors. In the base case we need to obtain the subgroups of simple groups which we can do either with the traditional method of cyclic extension [Neu60], or simply use the large amount of theoretical information available, such as [Pfe97].

## 4. SUBGROUPS OF A TRIVIAL-FITTING GROUP

We now assume again that $H$ is a Trivial-Fitting group with socle $S = \mathrm{Soc}(H) \lhd H$. We assume that we have determined the $S$-classes of subgroups of $S$, using the methods

of the previous section. We aim to extend this list to a list of representatives of the $H$-classes of subgroups of $H$. (The process of extension shares some similarities with [NP12].)

First consider subgroups of $S$: The action of $H$ can fuse $S$-classes of subgroups, as $S \lhd H$ the $S$-classes of subgroups form blocks for the action of $H$. If $U \leq S$ is such a subgroup then

$$b = \frac{[H:N_H(U)]}{[S:N_S(U)]} = \frac{[H:S]}{[N_H(U):N_S(U)]} \leq [H:S]$$

is a bound for the number of blocks. By computing $N_H(U)$ in a backtrack search we obtain $b$. If $b > 1$ the fusion of $S$-classes of subgroups to $H$-classes then can be done by an orbit algorithm [HEO05, Section 4.5.2] on blocks, given by representatives. In this, if $U_i$ is a representative of an $S$-class, and $h \in H$, we determine the $S$-class of $U_i^h$ and find $s \in S$ such that $U_i^{hs}$ is the chosen representative of its $S$-class.

We thus obtain representatives of the $H$-classes of subgroups in $S$.

Now consider an arbitrary subgroup $V \leq H$. Then $U = V \cap S \lhd V$ and clearly $U \leq S$ and $V \leq N_H(U)$. Conjugates of $V$ lead to conjugates of $U$, so it is sufficient to consider $U$ up to $H$-conjugacy. We shall classify all subgroups $V$ that intersect with $S$ in the same subgroup $U$, up to conjugacy with $N_H(U)$:

Let $\varphi\colon N_H(U) \to N_H(U)/N_S(U)$. As $\varphi$ is the restriction of the natural homomorphism $H \to H/S$ with domain restricted to $N_H(U)$ this can be constructed easily. Let $A := N_S(U) \cdot V$. Then $A^\varphi \leq N_H(U)^\varphi =: Q$. We obtain candidates for $A$ up to conjugacy in $N_H(U)$ by determining representatives of the classes of subgroups of $Q$. This group $Q$ in general is comparatively small (its order is again bounded by $[H:S]$) and often has a nontrivial radical (from the factors $\mathrm{Aut}(T_i)/T_i$, so the standard methods mentioned in the introduction work well.

We now shall classify all subgroups $V$ that lead to the same $U$ and the same $A$. As we permit conjugacy of $N_H(U)$, we shall consider $A$ only up to $N_H(U)$ conjugacy. These classes of subgroups are in bijection with the $Q$-classes of subgroups of $Q$. Let $A/N_S(U)$ be one such subgroup and let $M = N_{N_H(U)}(A) = N_H(U) \cap N_H(A)$. Then (figure 1) we have that $V/U$ is a complement to $N_S(U)/U$ in $A/U$, and every such complement gives a subgroup $V$ with the desired properties.

We can obtain these classes of complements by first determining the classes of complements under $A/U$ conjugacy and then fusing representatives under conjugacy by $N_H(U)$. (As in general $A \not\lhd N_H(U)$ this requires explicit conjugacy tests.) The representatives obtained are representatives of the desired subgroups $V$ up to conjugacy in $H$.

The algorithm for all subgroups then consists of:

1. Take representatives $U$ of the $H$ classes of subgroups of $H$.
2. For each such $U$ take representatives $A$ of the subgroups of $N_H(U)$, containing $N_S(U)$.
3. For each pair $U, A$ find subgroups $V$ as complements, fused under the action of $N_H(U)$.

If $N_S(U)/U$ is solvable the complements can be obtained with cohomological methods, see [CNW90] and [HEO05, Section 7.6.2], using a presentation for $A/N_S(U)$. (Such a presentation can be obtained for example using the methods of [BGK+97].)

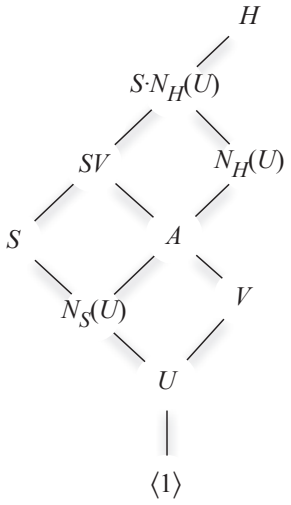


**Figure 1: Subgroups in $N_H(U)$**

In the situation considered here the group $N_S(U)/U$ often is not solvable. An example of such a situation (which also indicates why it occurs frequently) is if $U$ projects trivially on some direct factors of $S$. In this case all elements in thes (nonsolvable) direct factors then normalize $U$ and thus contribute to $N_S(U)/U$.

In many cases however the factor group $N_H(U)/N_S(U)$ (and thus the group $A/N_S(U)$) is solvable. This is for example the case if $U$ never has the same projection on more than four components (as $S_4$ is solvable) in particular if each $n_i \leq 4$.

We thus describe in section 5 a specific method to find classes of complements in the case of a solvable factor group. Section 6 then describes the general case.

# 5. COMPLEMENTS: SOLVABLE FACTOR GROUP

In this self-contained section we study the following situation (variables are not related to their use in the previous sections):

We are given a finite group $G$ and $N \lhd G$ such that $N$ is arbitrary but $G/N$ is solvable. We want to determine, up to $G$-conjugacy, the subgroups $C \leq G$ such that $C \cap N = \langle 1 \rangle$ and $NC = G$.

As we actually need to determine complements in a factor group, we consider a slightly generalized situation (see figure 2):

DEFINITION 2. *Given a group $G$ and $N, M \lhd G$, we say that that a subgroup $M \leq C \leq G$ complements $N$ in $G$ modulo $M$ if $NMC = G$ and $NM \cap C = M$.*

We assume that $G/NM$ is solvable and want to determine these subgroups up to conjugacy by $G$.

Since we assumed that $G/NM$ is solvable, there exists a normal subgroup $NM \leq A \lhd G$ such that $A/NM$ is a $p$-group for some prime $p$. Clearly any complement $C$ in $G$

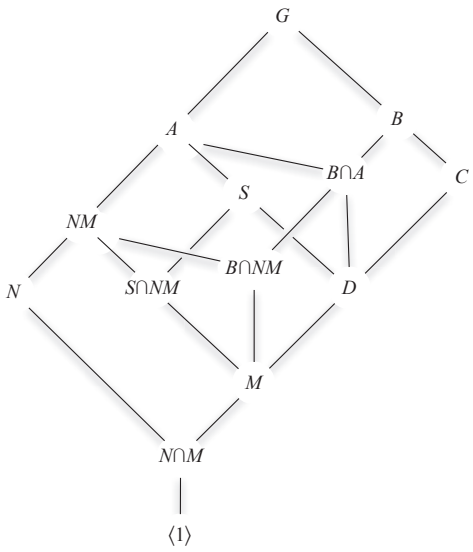


**Figure 2: Complements in the factor group**

must contain a normal subgroup $D = C \cap A$, this group $D$ is a complement to $NM$ in $A$ modulo $M$. As $D/M \cong A/NM$ is a $p$-group, by the 2nd Sylow theorem we can assume – up to conjugacy – that any such complement $D$ lies in $S$, where $S/M$ is a particular $p$-Sylow subgroup of $A/M$. Thus $D$ is a complement to $S \cap NM$ in $S$ modulo $M$.

Given such a complement $D$, we known that $C \leq B := N_G(D)$ and thus that $N \cdot B = G$. Furthermore $C \cap A = D$, thus $C$ is a complement to $B \cap A$ in $B$ modulo $D$.

This motivates the following strategy, given $G, N, M$:

1. Determine a subgroup $A \geq N$, $A \lhd G$, such that $A/NM$ is a $p$-group for some prime $p$. (See below on how to construct $A$.)

2. Determine (for example using [CCH97]) a $p$-Sylow subgroup $P \leq A$, let $S = MP$. (So $[S{:}M] = p^x$.)

3. Using cohomology [CNW90], compute representatives of the conjugacy classes of complements to $S \cap NM$ in $S$ modulo $M$. Determine representatives of the $G$-classes of these complements. (This is done best by first fusing under the action of $N_G(S)$ which is an action on the cohomology group, followed by conjugacy tests in $G$.)

   The groups obtained in this step are representatives of the classes of complements to $N$ in $A$ modulo $M$, as every complement is $G$-conjugate to a complement in $S$.

4. For each such complement $D$ determine $B := N_G(D)$ and check whether $N \cdot B = G$. If not discard $D$ as its normalizer may not contain a complement to $N$ in $G$.

5. Otherwise work recursively in $B$ and compute $B$-classes of complements $C$ to $B \cap A$ modulo $D$.

By the above argument clearly any complement to $N$ modulo $M$ is conjugate to one of the groups $C$ in this classification. We can ensure that no duplicates are constructed if $A/NM$ is characteristic (i.e. invariant under all automorphisms) in $G/NM$:

LEMMA 3. *Assume (notation as in the algorithm above) that $A/NM$ is characteristic in $G/NM$. Let $\{D_i\}$ be a set of representatives of $G$-classes of complements to $N$ in $A$ modulo $M$ such that $N \cdot N_G(D_i) = G$, and for each $i$ let $\{C_{i,j}\}$ be a set of the $N_G(D_i)$-classes of complements to $N \cap N_G(D_i)$ modulo $D_i$. Then every subgroup $C$ complementing $N$ modulo $M$ in $G$ is conjugate to exactly one $C_{i,j}$.*

PROOF. The argument above already establishes that every subgroup $C$ with the given properties is conjugate to at least one of the $C_{i,j}$.

Assume conversely that two of the $C_{i,j}$, call them $C_1$ and $C_2$ are conjugate: $C_1^g = C_2$, and that they were obtained from subgroups $D_1$, respectively $D_2$. The natural homomorphism $G/M \to G/NM$ induces isomorphisms $\phi_i \colon C_i/M \to G/NM$ such that $D_i/M^{\phi_i} = A/NM$.

If $D_1^g = D_2$ then $D_1 = D_2$ by the choice of the $D_i$ and $g \in N_G(D_1)$, contradicting the choice of the $C_{1,j}$ to be representatives under the action of $N_G(D_1)$.

Otherwise consider the isomorphism $\phi \colon G/NM \to G/NM$ given by $x \mapsto ((x^{\phi_1^{-1}})^g)^{\phi_2}$. We then have that $A^\phi \neq A$, contradicting the choice of $A$ being characteristic. □

## 5.1 Choice of normal subgroups

We finally just need to describe how to construct the subgroup $A$ that leads to a characteristic factor $A/NM$. For this we are using standard methods for solvable groups.

DEFINITION 4 ([CELG04]). *Let $G$ be a finite solvable group. The elementary abelian nilpotent-central (EANC) series*

$$G = G_1 \rhd G_2 \rhd \cdots \rhd G_{m+1} = \langle 1 \rangle$$

*is obtained by iteratively refining normal series of $G$:*

1. *Start with a series*

   $$G = N_1 \rhd N_2 \rhd \cdots \rhd N_{m+1} = \langle 1 \rangle$$

   *such that $N_{i+1}$ is minimal normal in $N_i$ such that $N_i/N_{i+1}$ is nilpotent.*

2. *Consider each nilpotent factor as a direct product of $p$-groups. For each direct factor take the lower exponent $p$-central series, take the direct products for all primes of subsequent factors of these series (thus the factors are direct products of elementary abelian $p$-groups).*

3. *Refine each of these factors by taking the series given by direct products of $p$-Sylow subgroups in order of ascending $p$.*

*It is shown in [CELG04] that the subgroups in this series are characteristic and the subsequent factors are elementary abelian $p$-groups.*

Efficient methods for computing this series are given in [CELG04] as well.

We thus choose $A$ such that $A/NM$ is the lowest nontrivial factor in the EANC series of $G/NM$. As we recurse only if $BNM = G$, the EANC series of $B/B \cap NM$ corresponds to the EANC series of $G/NM$. Furthermore (by the definition) we have that for a subgroup $G_i \lhd G$ in the EANC series we have that in the EANC series for $G/G_i$ consists of the groups $G_j/G_i$ for $j \leq i$.

Therefore this series needs to be computed only once and the subsequent factors can be used in the recursion.

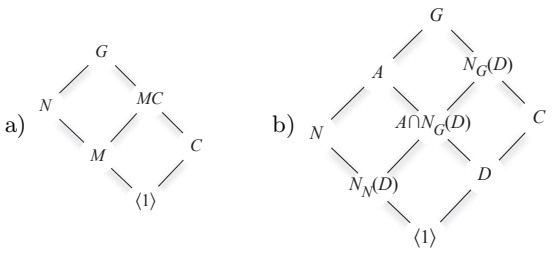


**Figure 3: General Complement Situation**

| Group | Order | Classes | time | cyclic ext. |
|---|---|---|---|---|
| $S_5 \wr S_2$ | 28800 | 561 | 24 | 10 |
| $S_5 \times S_6$ | 86400 | 3182 | 162 | 163 |
| $S_5 \times S_7$ | 604800 | 5913 | 277 | 1441 |
| $U_3(5).S_3$ | 756000 | 244 | 43 | 287 |
| $S_6 \wr S_2$ | 1036800 | 8147 | 299 | 3745 |
| $S_5 \wr S_3$ | 10368000 | 29155 | 1913 | 261561 |
| $U_4(3).D_8$ | 26127360 | 3870 | 5245 | 319124 |
| $M_{11} \wr S_2$ | 125452800 | 2048 | 367 | - |
| $S_6 \wr S_3$ | 2239488000 | 7172632 | 680966 | - |

**Table 1: Some run times of the algorithm**

## 6. COMPLEMENTS: GENERAL CASE

We finally briefly describe the general situation of determining classes of complements to a normal subgroup $N \lhd G$. The methods from [CNW90] as well as from [CH04, Section 4] and from section 5 indicate the following two reductions (see figure 3) for the problem:

**a)** If there is $M \lhd G$, $M \leq N$, any complement $C$ to $N$ will have $MC/M$ complement $N/M$ in $G/M$. Furthermore $C$ complements $M$ in $MC$. Thus first find classes of complements to $N/M$ in $G/M$ and then for each subgroup $D \geq M$ such that $D/M$ is representative of a class of complements find complements to $M$ in $D$. Fuse under action of $N$.

**b)** If there is $A \lhd G$, $N \leq A$, then any complement $C$ to $N$ in $G$ will contain a subgroup $D \lhd C$ complementing $N$ in $A$ and $C \leq N_G(D)$. Thus first find complements to $N$ in $A$, fuse under the action of $G$. Then for each such complement $D$ such that $N \cdot N_G(D) = G$, work in $N_G(D)$: Let $Z = A \cap N_G(D) = D \cdot N_N(D)$ and find complements to $Z/D$ in $N_G(D)/D$. Every complement $C$ arises this way, if $A/N$ is characteristic in $G/N$ the argument from lemma 3 shows that no further fusion under action of $G$ can take place.

Thus the only remaining case in which neither reduction applies is applicable, nor normal subgroup nor factor group are solvable is that of $N$ elementary nonabelian and $G/N$ simple. The paper [CH04, Section 4] suggests in this case a reduction to maximal subgroups which it acknowledges as a not very efficient method.

In our situation however this means that for at least five projections $T_i$ the quotient $N_S(U)/U$ must have a nonsolvable projection image and that these components are permuted transitively. This means that the whole group $H$ already must be rather large and a calculation currently will likely already face obstacles of memory requirements for storing the subgroups. Thus this issue of complements, while being a theoretical problem, is it less of a practical concern here.

## 7. IMPLEMENTATION

The algorithm as described has been implemented by the author in GAP [GAP13] and is available in release 4.6 of the system. (The complement routine of section 5 is already available in release 4.5.) Table 1 shows the performance in comparison with the cyclic extension algorithm used by default. (For the base case of simple groups the new algorithm still used cyclic extension, and not table lookup, to get the classes of subgroups. Doing so would have given a further speedup.) All groups were represented by permutations in the smallest degree possible. Column "time" is the time taken by this new algorithm, column "cyclic extension" the timing for the default cyclic extension algorithm.

Runtimes are in seconds on an 2.3 GHz AMD Opteron 6276 under Linux with ample memory to allow storage of all subgroups. In the case of $M_{11} \wr S_2$ the cyclic extension algorithm was provided with a list of all perfect subgroups, obtained from the prior subdirect product calculation for $M_{11} \times M_{11}$, but still did not finish in weeks. The calculation for $S_6 \wr S_3$ by cyclic extension is absolutely hopeless.

It is easily seen that the new algorithm is an improvement except for the smallest cases. One reason for this is the large number of conjugacy tests the cyclic extension algorithm needs to do to eliminate duplicates.

## 8. ACKNOWLEDGMENTS

Experimental runs on large groups were aided substantially by the checkpointing facility of the DMTCP [AAC09] project that allowed to restart calculations after a reboot. The author's work has been supported in part by Simons Foundation Collaboration Grant 244502 which is gratefully acknowledged.

## 9. REFERENCES

[AAC09] Jason Ansel, Kapil Arya, and Gene Cooperman. DMTCP: Transparent checkpointing for cluster computations and the desktop. In *23rd IEEE International Parallel and Distributed Processing Symposium*, Rome, Italy, May 2009.

[BB99] László Babai and Robert 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.

[BEO02] Hans Ulrich Besche, Bettina Eick, and E. A. O'Brien. A millennium project: constructing small groups. *Internat. J. Algebra Comput.*, 12(5):623–644, 2002.

[BGK+97] László Babai, Albert J. Goodman, William M. Kantor, Eugene M. Luks, and Péter P. Pálfy. Short presentations for finite groups. *J. Algebra*, 194:97–112, 1997.

[Can11] John Cannon. Problems I would like to solve in

CGT. *Oberwolfach Reports*, 8(3):2127–2128, 2011.

[CCH97] John J. Cannon, Bruce C. Cox, and Derek F. Holt. Computing Sylow subgroups in permutation groups. *J. Symbolic Comput.*, 24(3-4):303–316, 1997. Computational algebra and number theory (London, 1993).

[CCH01] John Cannon, Bruce Cox, and Derek Holt. Computing the subgroup lattice of a permutation group. *J. Symbolic Comput.*, 31(1/2):149–161, 2001.

[CELG04] John J. Cannon, Bettina Eick, and Charles R. Leedham-Green. Special polycyclic generating sequences for finite soluble groups. *J. Symbolic Comput.*, 38(5):1445–1460, 2004.

[CH04] John Cannon and Derek Holt. Computing maximal subgroups of finite groups. *J. Symbolic Comput.*, 37(5):589–609, 2004.

[CNW90] Frank Celler, Joachim Neubüser, and Charles R. B. Wright. Some remarks on the computation of complements and normalizers in soluble groups. *Acta Appl. Math.*, 21:57–76, 1990.

[Fei80] Walter 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.

[GAP13] The GAP Group, `http://www.gap-system.org`. *GAP – Groups, Algorithms, and Programming, Version 4.6.3*, 2013.

[HEO05] Derek F. Holt, Bettina Eick, and Eamonn A. O'Brien. *Handbook of Computational Group Theory*. Discrete Mathematics and its Applications. Chapman & Hall/CRC, Boca Raton, FL, 2005.

[Hol91] D. F. Holt. The computation of normalizers in permutation groups. *J. Symbolic Comput.*, 12(4-5):499–516, 1991. Computational group theory, Part 2.

[Hol10] Derek F. Holt. Enumerating subgroups of the symmetric group. In *Computational group theory and the theory of groups, II*, volume 511 of *Contemp. Math.*, pages 33–37. Amer. Math. Soc., Providence, RI, 2010.

[HP89] Derek F. Holt and W. Plesken. *Perfect groups*. Oxford University Press, 1989.

[Hul96] Alexander Hulpke. *Konstruktion transitiver Permutationsgruppen*. PhD thesis, Rheinisch-Westfalische Technische Hochschule, Aachen, Germany, 1996.

[Hul05] Alexander Hulpke. Constructing transitive permutation groups. *J. Symbolic Comput.*, 39(1):1–30, 2005.

[Hular] Alexander Hulpke. Computing conjugacy classes of elements in matrix groups. *J. Algebra*, to appear.

[Leo97] Jeffrey S. Leon. Partitions, refinements, and permutation group computation. In Larry Finkelstein and William M. Kantor, editors, *Proceedings of the 2nd DIMACS Workshop held at Rutgers University, New Brunswick, NJ, June 7–10, 1995*, volume 28 of *DIMACS: Series in Discrete Mathematics and Theoretical Computer Science*, pages 123–158. American Mathematical Society, Providence, RI, 1997.

[Mon12] Kenneth Monks. *The Moebius Number of the Symmetric Group*. PhD thesis, Colorado State University, Fort Collins, CO, 2012.

[Neu60] Joachim Neubüser. Untersuchungen des Untergruppenverbandes endlicher Gruppen auf einer programmgesteuerten elektronischen Dualmaschine. *Numer. Math.*, 2:280–292, 1960.

[NP12] L. Naughton and G. Pfeiffer. Computing the table of marks of a cyclic extension. *Math. Comp.*, 81(280):2419–2438, 2012.

[Pfe97] Götz Pfeiffer. The subgroups of $M_{24}$, or how to compute the table of marks of a finite group. *Experiment. Math.*, 6(3):247–270, 1997.

[Rem30] Robert Remak. Über die Darstellung der endlichen Gruppen als Untergruppen direkter Produkte. *J. Reine Angew. Math.*, 163:1–44, 1930.

[Sha97] John Shareshian. On the Möbius number of the subgroup lattice of the symmetric group. *J. Combin. Theory Ser. A*, 78(2):236–267, 1997.

[The97] Heiko Theißen. *Eine Methode zur Normalisatorberechnung in Permutationsgruppen mit Anwendungen in der Konstruktion primitiver Gruppen*. Dissertation, Rheinisch-Westfalische Technische Hochschule, Aachen, Germany, 1997.