J. Symbolic Computation (2000) **11**, 1–000

Computing Subgroups Invariant Under a Set of Automorphisms

ALEXANDER HULPKE

School of Mathematical and Computational Sciences, University of St Andrews, U.K.

(Received 17 August 2000)

This article describes an algorithm for computing up to conjugacy all subgroups of a finite solvable group that are invariant under a set of automorphisms. It constructs the subgroups stepping down along a normal chain with elementary abelian factors.

1. Introduction

When examining the structure of a finite group G, a typical question is the determination of the conjugacy classes of subgroups. For this problem a well-known algorithm – the cyclic extension method (Neubüser 1960, Mnich 1992) – has been in use for over 30 years. For practical purposes this algorithm is limited to groups of size a few thousand. If the subgroup lattice is very thin the possible size may be increased by another factor of ten. Problems appear, however, as soon as higher-dimensional vector spaces occur as subfactors of the group. In this situation the plain multitude of subgroups just overwhelms the algorithm.

On the other hand, quite often a user is not interested in all subgroups (or conjugacy classes thereof) but only in those with special properties. A typical example are maximal subgroups, which can be computed quite efficiently in solvable groups (Eick 1993, Cannon and Leedham-Green).

In contrast, we want to determine the subgroups that are invariant under a subgroup $\Phi \leq \mathrm{Aut}(G)$ of automorphisms.

Our motivation for considering this problem comes from the task of constructing all permutation groups of a given degree (Hulpke 1996), where under certain circumstances the process of constructing possible base groups boils down to the determination of subgroups of a direct power invariant under permutation of the components.

Another application might be the determination of all normal subgroups of a group contained in a given solvable normal subgroup of the group (Hulpke 1998).

For an elementary abelian group G this problem specializes to the determination of all Φ-submodules. For this task efficient algorithms are known (Lux *et al.* 1994) that we can use as building blocks.

Our strategy will be to construct the subgroups iteratively via homomorphic images: Let $G = N_0 > N_1 > \cdots > N_r = \langle 1 \rangle$ be a series of Φ-invariant normal subgroups of G. We construct the subgroups of G/N_i based on the knowledge of the subgroups of G/N_{i-1},

0747–7171/90/000000 + 00 $03.00/0

starting with the trivial factor group G/G. We will limit ourselves to the consideration of solvable groups because for these each factor N_{i-1}/N_i can be chosen to be elementary abelian.

In this situation in each step the subgroups of G/N_i can be considered as extensions of elementary abelian normal subgroups. This case of extensions is described by cohomology theory that we will briefly recall in the next section, closely following (Celler *et al.* 1990). For the sake of simplicity before describing the general algorithm we then describe the special case of a trivial operation ($\Phi = \langle 1 \rangle$), namely the determination of conjugacy classes of all subgroups. Similar algorithms to the one described there have also been suggested by Slattery and Cannon *et al.*.

The following section then describes the general case of a nontrivial Φ. We finish the description with some remarks towards efficiency and implementational issues.

2. Cohomology of extensions

Within this section the group E shall be an extension of the elementary abelian normal subgroup $M \lhd E$ with the factor group $F = E/M$. We denote the natural homomorphism $E \to F$ by $e \mapsto \bar{e}$. As M is abelian, the mapping $F \to \mathrm{Aut}(M)$, $f \mapsto (m \mapsto m^{f\tau})$, where τ is any section $F \to E$, is well defined (and independent of τ). We set

$$Z^1(F,M) := \{\gamma\colon F \to M \mid (fg)\gamma = (f\gamma)^{g\tau}(g\gamma) \text{ for all } f,g \in F\} \tag{2.1}$$

the group of *1-Cocycles* and

$$B^1(F,M) := \{\gamma_m = (f \mapsto m^{-f}m)\colon F \to M \mid m \in M\}$$

the group of *1-Coboundaries*. It is easily checked that B^1 is a subgroup of Z^1.

Provided the extension E splits over M and $G \leq E$ is a fixed complement, every complement of M in E is of the form $\{g(\bar{g}\gamma) \mid g \in G\}$ for one $\gamma \in Z^1$. Two complements corresponding to cocycles $\gamma, \delta \in Z^1$ are conjugate in E if and only if the quotient γ/δ is contained in B^1. Thus the factor group $H^1 = Z^1/B^1$ is in one-to-one correspondence to the conjugacy classes of complements of M in E.

As shown in (Celler *et al.* 1990), finding one complement to M is equivalent to finding one solution of an inhomogeneous system of linear equations in the vector space M, the corresponding homogeneous system determines Z^1. Its subgroup B^1 can be computed straight from the definition.

2.1. Action on Complements

We will now suppose that E splits over M. Let $\varphi \in \mathrm{Aut}(E)$ be an automorphism which leaves M set-wise invariant. Then φ permutes the complements of M. This induces an action on the conjugacy classes of complements. As these classes are in bijection to H^1 we get in turn an action on H^1. This action will be described this section.

Let $G \leq E$ again be a fixed complement. We denote by ϕ the action induced by φ on G by identification of G with F via the natural homomorphism $E \to F$. It is defined by $(gM)\varphi =: (g\phi)M$, that is $\bar{g}\varphi = \overline{g\phi}$. For $g \in G$ we set $m_{g,\varphi} := (g\phi)^{-1}g\varphi \in M$.

We will define the action of φ on H^1 by defining the images for representatives in Z^1: Let $\gamma \in Z^1$ and $G_\gamma := \{g \cdot \bar{g}\gamma\}$ the corresponding complement to M. As φ fixes M, the image G_γ^φ is another complement to M. It consists of the elements

$$(g(\bar{g}\gamma))\varphi = g\varphi \cdot (\bar{g}\gamma)\varphi = g\phi m_{g,\varphi} \cdot (\bar{g}\gamma)\varphi = g\phi \cdot \overline{(g\phi)}\delta_\gamma, \tag{2.2}$$

where we define $\delta_\gamma: F \to M$ via

$$\bar{g}\delta_\gamma := m_{g(\phi^{-1}),\varphi}(\overline{g(\phi^{-1})}\gamma)\varphi.$$

As ϕ maps G onto G we see that the complement G_γ^φ consists of elements of the form $g\bar{g}\delta_\gamma$. This implies that δ_γ fulfills the condition in (2.1) and thus is a 1-cocycle.

Accordingly, we define an action of φ on H^1 by $(B^1\gamma)\varphi := B^1\delta_\gamma$. This action is not necessarily linear (B^1 need not remain fixed) but affine. It permutes the classes in H^1 in the same way the complement classes are permuted by φ. Representatives of the orbits are representatives of the φ-fused classes of complements.

To perform this action on H^1 in practice, we consider Z^1 as a space of row vectors and identify H^1 with a fixed complement space to B^1 (by computing a basis of B^1 in echelon form) The actual action on H^1 then consists of action on the representatives according to (2.2) followed by projection to the selected complement space.

2.2. Invariant Complements

Again, we consider the situation of an automorphism φ of E that leaves the normal subgroup $M \lhd E$ invariant. Instead of looking at the action of φ on the classes of complements we look at the action on single complements and ask for orbits of length one, that is, complements which are invariant under φ.

However, we only want to get representatives of these subgroups up to E-conjugacy. So we search for one invariant complement within each conjugacy class of complements. While a set of representatives of H^1 will get us representatives of the conjugacy classes of complements, the choice of representatives (implicitly done by selecting cocycles as representatives) might select a complement not invariant under φ whereas another complement in the same G-class is invariant under φ. We want to check whether this might be the case, at the same time exposing the invariant conjugate.

Let $K \leq E$ be a complement to M in E, corresponding to the cocycle γ with respect to a fixed complement G. (That is, $K = G_\gamma$.) Then K is of the form $\{g \cdot \bar{g}\gamma \mid g \in G\}$. As K normalizes itself it is sufficient to conjugate by elements of M. Conjugating the element $g \cdot \bar{g}\gamma$ with $m \in M$ yields the image

$$g^m \cdot \bar{g}\gamma = g \cdot [g, m] \cdot \bar{g}\gamma,$$

using the fact that M is abelian. The invariance of a conjugate of K under φ thus implies that for every $g \in G$, there is an $h \in G$ such that

$$(g[g, m] \cdot \bar{g}\gamma)\varphi = h[h, m] \cdot \bar{h}\gamma \tag{2.3}$$

holds. Using the induced action on E/M we see $\bar{g}\varphi = \bar{h}$, thus $g\varphi = hn$ with $n \in M$. Accordingly, we can translate (2.3) to

$$hn[hn, m\varphi] = h[h, m] \cdot \bar{h}\gamma/\bar{g}\gamma\varphi, \text{ respectively } n[hn, m\varphi] = [h, m] \cdot \bar{h}\gamma/\bar{g}\gamma\varphi.$$

As M is elementary abelian, n, $m\varphi$ and the commutators commute. Thus we obtain

$$n[h, m\varphi] = [h, m] \cdot \bar{h}\gamma/\bar{g}\gamma\varphi.$$

Writing this additively as an equation in M we get

$$n - m\varphi' h' + m\varphi' = -mh' + m + (\bar{h}\gamma - \bar{g}\gamma\varphi),$$

denoting by h' and φ' the induced linear mappings of the vector space M. Thus the

conjugating element m we look for is a solution of the system of linear equations:

$$m(1-h'+\varphi' h'-\varphi') = n-(\bar{h}\gamma-\bar{g}\gamma\varphi) \qquad \forall g\in G. \tag{2.4}$$

Conversely, any solution of (2.4) leads to an invariant complement. As φ permutes the complements, it is sufficient that a set of generators of K (chosen by g running through a set of generators of G) is mapped by φ into K. We have seen:

LEMMA 2.1. *Let $\Phi \le Aut(E)$ be a group of automorphisms, fixing $M \lhd E$. Let M be elementary abelian and G a fixed complement to M. If K is a complement to M, corresponding to the cocycle γ, then there is a conjugate of K, invariant under Φ if and only if the system of equations*

$$m(1-h'+\varphi' h'-\varphi') = n-(\bar{h}\gamma-\bar{g}\gamma\varphi), \qquad g\varphi = hn \qquad (h\in G, n\in M)$$

with g running through a generating set of G and φ through a generating set of Φ has a nontrivial solution m. This solution is a conjugating element.

A nice observation is that the corresponding homogeneous system is independent of the choice of the cocycle γ. Using standard LR-decomposition techniques thus only one Gaussian elimination has to be performed for all complement classes simultaneously.

3. Trivial Action

In this section we shall describe an algorithm for the computation of conjugacy classes of subgroups of a solvable group G. In the subsequent section this algorithm will then be generalized to yield only representatives of subgroups invariant under a set of automorphisms.

As described in the introduction we proceed inductively over a normal series $G \ge N_1 \ge \cdots \ge N_r$ with elementary abelian factors, in each step constructing the subgroups of the factors G/N_i from the subgroups of G/N_{i-1}.

By induction it is sufficient to consider a single step: Let $N \lhd G$ be an elementary abelian normal subgroup.

Consider an arbitrary subgroup $U \le G$. Then three possibilities for the relative locations of U and N are possible:

1 U contains N and thus is the full preimage of a subgroup of G/N.
2 U is contained in N and thus is a subspace of the vector space N.
3 $B := N \cap U$ is a proper subgroup of N and $A := \langle N, U\rangle$ is a subgroup containing N properly.

We will get subgroups of type 1 as preimages of subgroups of G/N and subgroups of type 2 as subspaces of the vector space N. So it is sufficient to consider subgroups of the third kind:

In this case, B is normal in U (because it is the intersection of U with a normal subgroup) and in N (because N is abelian). Thus B is normal in $\langle N, U\rangle = A$ and $C := N_G(A) \cap N_G(B)$ contains A. Finally, U/B is a complement to N/B in A/B. Figure 1 illustrates the situation.

As N is normal in G, we have

$$N_G(U) \le N_G(B) \qquad \text{and} \qquad N_G(U) \le N_G(A). \tag{3.1}$$

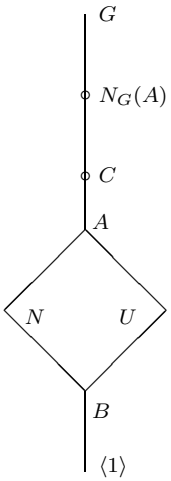

Figure 1. subgroup lattice structure

Provided we know all subgroups properly containing N and all subgroups of N, every subgroup of G not contained in one of those two sets can be obtained as a complement to N/B in A/B where $B \leq N \leq A$, $B \lhd A$ holds.

As we want to obtain representatives up to conjugacy, we now consider two conjugate subgroups $U, U' \leq G$. Then $A = \langle N, U\rangle$ and $A' = \langle N, U'\rangle$ are conjugate in G as well. If $A = A'$ holds, the subgroups $B = N \cap U$ and $B' = N \cap U'$ are conjugate under $N_G(A)$. If even $B = B'$ holds, U and U' are conjugate under $C = N_G(B) \cap N_G(A) \geq A$. Thus U/B and U'/B are complements to N/B in A/B, conjugate under C/B.

Finally we note how to get representatives of the G-classes from this:

LEMMA 3.1. *Let $N \lhd G$ be an elementary abelian normal subgroup, $\mathcal{A}$ a set of representatives of the conjugacy classes of those subgroups of G that contain N properly and $\mathcal{B}$ (containing N) a set of representatives of the G-classes of subgroups in N. For each $A \in \mathcal{A}$ let $\mathcal{B}_A$ be a set of representatives of the $N_G(A)$-classes of proper subgroups of N, that are normal in A. Finally, for $B \in \mathcal{B}_A$ set $C_{A,B} = N_G(A) \cap N_G(B)$ and let $\mathcal{U}_{A,B}$ be the full preimages of a set of representatives of the $C_{A,B}$-classes of complements to N/B in A/B. Then*

$$\mathcal{R} := \mathcal{A} \cup \mathcal{B} \cup \bigcup_{A \in \mathcal{A}} \bigcup_{B \in \mathcal{B}_A} \mathcal{U}_{A,B}$$

is a set of representatives for the G-classes of subgroups of G.

PROOF. The subgroups containing N or contained in N are conjugate to exactly one representative from $\mathcal{A}$ or $\mathcal{B}$. Thus we only need to consider subgroups $U \leq G$ of the third type.

If such a subgroup U is given, we might assume without loss of generality, that we have chosen a conjugate such that $A := \langle N, U\rangle$ is contained in $\mathcal{A}$. Then $B' = U \cap N$ is conjugate under $N_G(A)$ to a $B \in \mathcal{B}_A$. Again, we assume without loss of generality,

that $B = B'$ holds. Thus U/B is complement to N/B in A/B, respectively there is a $C_{A,B}$-conjugate of U such that $U \in \mathcal{U}_{A,B}$.

Conversely, above considerations show that U can be conjugate to at most one group from $\mathcal{R}$. □

We get $\mathcal{A}$ by taking full preimages of the subgroups of G/N that we assume to be known by induction. For the elementary abelian factor a simple base enumeration yields all subgroups. From these, we get $\mathcal{B}$ and the sets $\mathcal{B}_A$ by fusion under action of G, respectively action of $N_G(A)$. Usually, N is of small dimension and we don't lose any efficiency here.

As $B \leq U$ and $B \lhd C$, the normalizer $N_{C/B}(U/B)$ (that we get implicitly when fusing the complement classes) has the preimage $N_C(U)$ which according to (3.1) is equal to $N_G(U)$. These normalizers will be needed for the next iteration of the algorithm where U will play the role of an A.

To obtain representatives of the classes of complements we use the algorithm of (Celler *et al.* 1990) to find one complement together with the 1-Cohomology group. The action of C/B on the complements then is performed as given by (2.2).

As subgroups are constructed by *e*lementary *a*belian *e*xtension, this algorithm is baptized `eae`. We remark that the algorithm only needs solvability of N but not of G/N, thus generalization to groups with solvable normal subgroup is obvious.

As the construction process proceeds via factor preimages which grow in each step, every new step has to consider more groups for complement tests. On the other hand especially in the last step some properties of complements (for example the sizes) are known even before the complements are computed. Quite often, however, the user is interested only in some subgroups. For example the size might be restricted or prescribed exactly. In this case computation of complements can be skipped if the complements created would finally lead to subgroups not fulfilling the required properties. Similarly, if only subgroups with properties that will be preserved under homomorphisms (like being abelian or nilpotent) are desired, subgroups A for which the factor A/N does not fulfill these properties can be ignored for further lifting. For the special case of determining the normal subgroups of G further simplification is possible (Hulpke 1998).

4. Nontrivial Action

We now consider a nontrivial subgroup Φ of $\mathrm{Aut}(G)$ acting on a solvable group G. Our aim is to obtain the Φ-invariant subgroups of G up to conjugacy. For the sake of simplicity we consider G and Φ to be embedded into $G \rtimes \Phi$, thus letting Φ act by conjugation on G and allowing the multiplication of elements with automorphisms.

We shall apply this algorithm in cases in which the computation of the full subgroup lattice is impossible, thus we can not simply check which subgroups of the full lattice are Φ-invariant.

As noted above, for $U \leq G$, the invariance of U under Φ does not necessarily imply the Φ-invariance of conjugates U^g of U. Accordingly, we define:

Definition 4.1. *A* conjugacy class of Φ-invariant subgroups *consists of those subgroups of a conjugacy class that are invariant under* Φ.

We will consider these classes only if they are non-empty.

The general approach will be similar to the case of a trivial Φ: We first compute a

series of Φ-invariant normal subgroups with elementary abelian factors. These factors become Φ-modules. Section 4.2 explains how to do this.

To generalize the inductive step (lemma 3.1) we now consider the case of Φ acting on G and $N \lhd G$ being an Φ-invariant elementary abelian normal subgroup. Let U be a Φ-invariant subgroup of type 3 (that is neither contained in, nor containing N). Then $A = \langle N, U\rangle$ and $B = U \cap N$ are Φ-invariant as well.

LEMMA 4.1. *If $U \leq G$ is invariant under Φ then $N_G(U)$ is invariant under Φ as well.*

PROOF. Let $\varphi \in \Phi$ and $g \in N_G(U)$. Then

$$U^{(g\varphi)} = ((U\varphi^{-1})^g)\varphi = (U^g)\varphi = U,$$

thus $g\varphi \in N_G(U)$. □

Accordingly, $N_G(A)$,$N_G(B)$ and their intersection C are Φ-invariant as well and U/B is a complement to N/B invariant under the action induced on C/B.

If U and U' are conjugate and invariant under Φ, the corresponding groups A, A' and B, B' are conjugate to each other and Φ-invariant as well. Conversely however, conjugacy and invariance of A's and B's does not necessarily lead to conjugate invariant subgroups U and U', as the conjugate complements are not necessarily invariant again:

EXAMPLE 4.1. *Let*

$$G = S_4 = \langle (1,2,3,4), (1,2)\rangle \quad \textit{and} \quad N = V_4 = \langle (1,2)(3,4), (1,3)(2,4)\rangle \lhd G.$$

Let $\varphi \in Aut(G)$ be the inner automorphism induced by $(1,2)(3,4)$ and $\Phi = \langle\varphi\rangle \leq Aut(G)$. Then $G/N \cong S_3$ with φ acting trivially on G/N. The three 2-Sylow subgroups of the factor, $A_1/N = \langle N, (3,4)\rangle/N$, $A_2/N = \langle N, (1,3)\rangle/N$ and $A_3/N = \langle N, (2,3)\rangle/N$ thus are all invariant under the induced (trivial) automorphism of the factor. They form one conjugacy class. Let B be the trivial subgroup of G which is obviously invariant under φ. However, in A_1 there are two complements to N invariant under Φ, namely $\langle(1,2)\rangle$ and $\langle(3,4)\rangle$. They form one class of invariant complements. For A_2 and A_3 there are no such invariant complements. For example the corresponding conjugate subgroups of A_2 are $\langle(1,3)\rangle$ and $\langle(2,4)\rangle$, both not Φ-invariant.

Thus, when selecting representatives A and B it is not sufficient to search for invariant complements arising from this pair. In principle one has to consider complements from all possible pairs of conjugates of A and B, contradicting the idea of class representatives.

To overcome this problem we will instead consider "conjugated operations": If $U^g = g^{-1}Ug$ is invariant under Φ then obviously U is invariant under $g\Phi g^{-1} = \Phi^{g^{-1}}$. We call those images of the acting group (as we conjugate them with inverse elements) *jugated* images. Instead of searching for invariant conjugates of subgroups, we might check as well for subgroups invariant under jugated actions.

Accordingly, instead of conjugating A and B with a group element g to search for Φ-invariant complements arising from those conjugates, we can search for subgroups U arising as complements from A and B, for which there is a suitable $g \in G$ such that U is invariant under a jugated action $\Phi^{g^{-1}}$. Conjugating these complements back with g then leads to Φ-invariant subgroups.

While one might also hope that the number of jugated operations is less than the

number of conjugated subgroups (a reasonable hope if Φ is small or $\Phi = \mathrm{Inn}(G)$. In the latter case in fact there will be no jugated image of Φ which differs from Φ itself, as the inner automorphisms are invariant under themselves). The major advantage of this approach towards consideration of all conjugates is that we will not have to check invariant subgroups obtained by complement representatives for conjugacy in the whole group and can transfer the classification of lemma 3.1.

As we want to consider as few jugated operations as possible, we have to determine a minimal set of jugating elements g for a fixed pair $A \geq N$,$B \leq N$ such that searching for all $\Phi^{g^{-1}}$-invariant subgroups arising from A and B will yield a set of representatives of all Φ-invariant subgroups "belonging" to A and B (in the sense that for a trivial Φ a representative of its conjugacy class would be obtained as a complement to N/B in A/B).

4.1. Selecting Jugators

For a collection $\mathcal{C}$ of sets we denote by $\mathrm{ReprSet}(\mathcal{C})$ a set of representatives.

For any element $u \in N_G(\Phi)$ the elements g and gu lead to the same jugated action. So it is sufficient to consider one representative for each left coset from $G/N_G(\Phi)$. On the other hand, if we are interested in subgroups only up to K-conjugacy for a subgroup K of G, we just need to take one representative from each coset $K\backslash G$. That is:

$$\begin{aligned} &\exists_{h\in G}\,\exists_{k\in K} \quad (U^k \text{ invariant under } \Phi^{h^{-1}}) \\ &\quad\Leftrightarrow \quad \exists_{g\in \mathrm{ReprSet}(K\backslash G/N_G(\Phi))} \; V \text{ invariant under } \Phi^{g^{-1}} \quad \text{for a } V \in U^K. \end{aligned} \tag{4.1}$$

To restrict the number of cosets to be considered, we further observe that $\Phi^{g^{-1}}$-invariance of a group U implies the $\Phi^{g^{-1}}$-invariance of $A = \langle N, U\rangle$ and $B = N \cap U$. Only those elements are suitable jugators for which the chosen subgroups A and B are invariant under the jugated actions.

If A and B are chosen, conjugacy is restricted (that is, further conjugacy would move A or B) to $C_{A,B} = N_G(A) \cap N_G(B)$. As we are considering $C_{A,B}$-classes of complements at this stage, by (4.1) we just need to consider actions jugated with representatives from $C_{A,B}\backslash G/N_G(\Phi)$. This set of double cosets might be of substantial size, however, and we will try to reduce it by "factoring" the double cosets through $N_G(A)$: We may assume that

$$\begin{aligned} \mathit{reps} := \;& \mathrm{ReprSet}(C_{A,B}\backslash G/N_G(\Phi)) \\ & \subset \mathrm{ReprSet}(C_{A,B}\backslash N_G(A)) \cdot \mathrm{ReprSet}(N_G(A)\backslash G/N_G(\Phi)) \\ & =: \mathit{cosetprod}, \end{aligned} \tag{4.2}$$

with the set-wise product denoting the set of all products. Considering restrictions while determining *reps* from *cosetprod* will allow us to restrict the number of needed conjugates as early as possible, thus restricting the number of double cosets to be considered:

If we fix $A > N$, we restrict (con)jugacy to $N_G(A)$ and consider $N_G(A)$-classes of subgroups and double cosets from $N_G(A)\backslash G/N_G(\Phi)$. The condition of invariance of A further implies that we only consider such representatives $\{t_i\}$ from $\mathrm{ReprSet}(N_G(A)\backslash G/N_G(\Phi))$, for which A is invariant under $\Phi^{t_i^{-1}}$. But as conjugating subgroups is cheaper computationally than jugating mappings, we can test equivalently for A^{t_i} being invariant under Φ. From now on, t_i will always be assumed to fulfill this condition.

Now we have to determine those $B \leq N$ which are normal in A and invariant under at least one jugated action $\Phi^{t_i^{-1}}$. Therefore we determine all Φ-invariant subgroups of N (using the submodule algorithm from (Lux *et al.* 1994) if N is not a simple module) and select from their images under all t_i those which are normal in A. Afterwards we determine a set of representatives of the $N_G(A)$-classes of them.

Now we select a fixed representative B from this list and let $C = N_G(A) \cap N_G(B)$. By $\{s_j\}$ we denote a set of representatives for the right cosets $C\backslash N_G(A)$. Thus every product $s_j t_i$ determines a double coset from $C_{A,B}\backslash G/N_G(\Phi)$.

Every product $s_j t_i$ determines a conjugating element g up to C and $N_G(\Phi)$. As B has to be invariant under $\Phi^{(s_j t_i)^{-1}}$ it is sufficient to consider only those products $s_j t_i$ for which this invariance holds.

Finally we determine in the factor A/B complements to N/B which are invariant under the induced operation of at least one of these $\Phi^{(s_j t_i)^{-1}}$. This is done by computing the 1-Cohomology group and determining a set of representatives for all classes of complements. For each representative of the classes we check for the existence of a N/B-conjugate which is invariant under the induced action of one $\Phi^{(s_j t_i)^{-1}}$, using lemma 2.1 each time. If Bn is a suitable conjugating element in C/B, yielding the invariant complement U/B then $g = n s_j t_i$ is an element conjugating U to a Φ-invariant subgroup U' such that its closure $A' = \langle U', n \rangle$ and its intersection $B' = U' \cap N$ are conjugate to A and B respectively.

The complements obtained this way then have to be checked for "local" conjugacy under C/B. Taking representatives for the C/B-classes first before checking for invariant conjugates would yield no gain in performance because if we restrict the conjugation action from C to a normalizer $N_C(U)$ we would also need to consider further jugations with representatives from $N_C(U)\backslash C$, going from $C\backslash G/N_G(\Phi)$ to $N_C(U)\backslash G/N_G(\Phi)$. In other words: The reduction of candidates would have been made up by the need to consider further actions.

The representatives then finally are conjugated back by "their" conjugator $n s_j t_i$ to obtain Φ-invariant subgroups.

Vice versa, conjugating an Φ-invariant subgroup with a suitable $(s_j t_i)$ leads to a complement in a factor C/B invariant under the $s_j t_i$-jugated actions. Thus the described method yields representatives of all invariant subgroups. The above representatives are conjugate if and only if the corresponding complements belong to the same pair A, B and are conjugate under C/B. We have shown:

LEMMA 4.2. *Let $N \lhd G$ be abelian and invariant under Φ and let $\mathcal{A}$ be set of representatives of the Φ-invariant subgroups of G containing N. For each subgroup $A \in \mathcal{A}$ let $T_A := \{t_i\}$ be a set of representatives for the double cosets $N_G(A)\backslash G/N_G(\Phi)$, for which A is invariant under $\Phi^{t_i^{-1}}$:*

$$T_A = \left\{ x \in \mathit{ReprSet}(N_G(A)\backslash G/N_G(\Phi)) \mid A \text{ invariant under } \Phi^{x^{-1}} \right\}.$$

Further let $\mathcal{B}_A$ be a set of representatives of the $N_G(A)$-classes of subgroups properly contained in N, normal in A and invariant under a jugated action $\Phi^{t_i^{-1}}$ for (at least) one representative $t_i \in T_A$. For every $B \in \mathcal{B}_A$ let $\mathcal{U}_{A,B}$ be defined as in lemma 3.1.

For $B \in \mathcal{B}_A$ let $\{s_j\}$ be a set of representatives of the cosets $(N_G(A) \cap N_G(B))\backslash N_G(A)$ and

$$K_B = \{ s_j t_i \mid B \quad \text{invariant under} \quad \Phi^{(s_j t_i)^{-1}} \}.$$

For $U \in \mathcal{U}_{A,B}$ let

$$n_U := \begin{cases} ng & \text{if a } n \in N \text{ and a } g \in K_B \text{ exist, such that } U/B \text{ is invariant under } \Phi^{(ng)^{-1}}; \\ 0 & \text{otherwise.} \end{cases}$$

Finally, let $\mathcal{B}$ be a set of representatives of the G-classes of invariant subgroups in N. Then

$$\mathcal{R} := \mathcal{A} \cup \mathcal{B} \cup \bigcup_{A \in \mathcal{A}} \bigcup_{B \in \mathcal{B}_A} \bigcup_{\substack{U \in \mathcal{U}_{A,B} \\ 0 \neq n_U}} U^{n_U}$$

is a set of representatives of the G-classes of Φ-invariant subgroups.

As shown in (Laue 1982), the cosets given by $s_j t_i$ and $s_k t_l$ can be identical only if $t_i = t_l$ holds and s_j and s_k lie in the same orbit of $\mathrm{Stab}_{N_G(\Phi)}(N_G(A)t_i) = N_G(\Phi) \cap N_G(A)^{t_i} =: STC$. Thus, while considering the s_j and the t_i in the factorization given by (4.2) separately instead of considering only representatives for the double cosets $C_{A,B}\backslash G / N_G(\Phi)$ might lead to some double cosets considered twice, this can be dealt with by fusing the s_j under STC.

4.2. Obtaining an invariant series

To get an inductive algorithm from lemma 4.2 we need to obtain a Φ-invariant normal series for G with elementary abelian factors. Then the submodule algorithm from (Lux *et al.* 1994) yields for each normal factor all Φ-invariant submodules and the construction of all Φ-invariant subgroups of G proceeds as in the case of a trivial operation.

One possible solution is to use a characteristic series like the LG-series (Eick 1997). This section presents a different approach (which in some cases yields factors of higher dimension).

Lemma 4.3. *Let H be a group, $N \lhd H$ and $M \lhd N$ with $S := N/M$ simple. Then $L := \cap_{h \in H} M^h$ is normal in H and N/L is elementary of type S.*

Proof. As it is the intersection of an orbit of H, L is normal in H. By construction the factor group N/L is an iterated subdirect product of S. As S is simple, it has to be a direct product of groups isomorphic to S. Thus N/L is elementary. □

For a normal subgroup N of G we can easily get a subgroup $M \lhd N$ with $[N : M] = p$ a prime (for example take the first subgroup of a composition series). Then applying the above lemma with $H = G \rtimes \Phi$ yields a Φ-invariant normal subgroup $L \lhd G$ with N/L elementary abelian. Iterated application yields a series.

The normal subgroup obtained by the lemma is the largest possible subgroup contained in the given M. For practical purposes, however, it can be preferable to get larger factors. In this case one can start with a characteristic series (for example the derived series) and use lemma 4.3 only to refine non-elementary steps.

Table 1. Runtimes for the lattice computation

Group G	$\lvert G\rvert$		#Classes	t_{eae}	t_{ce}
$\frac{1}{2}[3^4 : 2^2]_c D_4 = T_{12} N_{209}$	1296	$= 2^4 3^4$	370	20	59
Borel($GL_3(4)$)	1728	$= 2^6 3^3$	298	48	58
$A_4 \times A_4 \times A_4$	1728	$= 2^6 3^3$	543	43	111
$N_{PGL_3(23)}(\text{Syl}_{11})$	2904	$= 2^3 3 \cdot 11^2$	43	6	10
Borel($SL_4(3)$)	5832	$= 2^3 3^6$	1867	211	639
$ThM11 = 7^2 : (3 \times 2S_4)$	7056	$= 2^4 3^2 7^2$	70	14	24
Borel($GL_2(41)$)	65600	$= 2^6 5^2 41$	592	116	575
Gl/N	165888	$= 2^{11} 3^4$	1488	590	17387
$Grp3$	5038848	$= 2^8 3^9$	7065	3541	—

The notation GMn indicates the n-th maximal subgroup of the almost simple group G. The group Gl is an iterated semidirect product constructed by Glasby (1989), it has a unique normal subgroup N of size 19683. The group $Grp3$ is an example constructed by Eick. For this group the cyclic extension algorithm did not finish in 128MB of memory.

5. Implementation

The described algorithms have been implemented by the author in GAP4 (GAP 1997) as the command `SubgroupsSolvableGroup`. (A similar function for the case of a trivial Φ is implemented in Magma (Bosma *et al.* 1997) by the command `SubgroupClasses`.) For computations in G we use a PC representation (Laue *et al.* 1984) which is adapted to the normal series of G used for the computation. Taking factor group images or preimage representatives is easy in this representation. For computing H^1 existing GAP code can be used.

It might be of interest to compare the performance of the described eae algorithm with the traditionally used cyclic extension code. Table 1 gives runtimes (seconds on a 200MHz PentiumPro under Linux) for a set of arbitrarily selected solvable groups. The eae code was implemented by the author, for cyclic extension the standard GAP library function `LatticeByCyclicExtension` was used. The performance times of eae appear to be favourable as soon as the groups get larger and the number of subgroups gets bigger. Thus it should be possible to examine the structure of groups a magnitude larger than before.

One reason for this seems to be that usually the major part of the subgroups consists of small subgroups which are constructed quite early in cyclic extension (and have to be kept track of afterwards), but only at the end of eae. Also eae seems to need less conjugacy tests and needs to keep only one conjugate of each class in memory, in contrast to cyclic extension which needs a complete list of so-called "zuppos" (cyclic subgroups of prime-power order).

On the other hand cyclic extension will cope happily with nonsolvable groups, provided representatives for all perfect subgroups are given, while eae cannot tackle those groups at all. Fortunately there is a multitude of interesting non-solvable groups which contain a solvable normal subgroup. For these groups one can compute the subgroup lattice of the nonsolvable (smaller) factor by cyclic extension and use eae which just needs solvability of the normal subgroup and not of the factor afterwards to obtain representatives of all subgroups. Though this strategy has yet to be tested thoroughly, it seems that this

Table 2. Runtimes for the restricted algorithm

G	$\lvert G\rvert$	Φ	Restriction	#Classes	t
S_3^7	$2^7 3^7$	Z_7	—	20	9
			$6 \mid$ Size	13	6
A_4^7	$2^{14}3^7$	Z_7	—	219	890
$3_+^{1+6} : 2^{3+4} : 3^2 : 2$ $= Fi_{22}M11$	$2^8 3^9$	—	Size=1944	159	1127
Gl	$2^{11}3^1 3$	Syl_2	—	258	4745
$3_+^{1+8} : 2_-^{1+6}.3_+^{1+2}.2S_4$ $= Fi_{23}M7$	$2^{11}3^{13}$	Syl_3	—	99	6575
$Fi_{23}M7$	$2^{11}3^{13}$	$U{=}\langle G.1, G.2, G.3\rangle, \lvert U\rvert = 11664$	—	579	22286

mixed approach will again allow to examine the subgroup structure of substantially larger groups. (The implementation described by Cannon *et al.* uses this approach.)

As mentioned in the introduction, similar algorithms have been suggested and implemented by Slattery and by Cannon *et al.*. Their observations agree with the preceding remarks.

We now turn to the second algorithm. While the major part of this algorithm's runtime is spent in the test for invariant complements, a crucial part of the current implementation is the construction of the semidirect product $G \rtimes \Phi$ needed to compute the normalizer of Φ and to jugate actions. In the cases considered, Φ itself has been solvable too. Thus the semidirect product can be constructed as an PC group again. In other cases a suitable representation for the semidirect product has to be found prior to the application of the algorithm.

According to (Slattery) the computation of double cosets in solvable groups also proceeds inductively via a normal chain with elementary abelian factors. Thus in each step the necessary double coset information can be lifted from the double cosets computed in the previous step.

As mentioned above, lifting can be restricted to construct only subgroups with certain properties. Examples (see table 2) show that this might increase the performance substantially.

A special case is normality of the subgroups in G (in other words: $\mathrm{Inn}(G) \leq \Phi$). In this case the search for complements can be restricted to normal complements, which are easier to compute as no conjugacy needs to be considered. This applies for example to the search for normal subgroups contained in a given normal subgroup.

Table 2 gives runtimes of the author's GAP implementation (again in seconds on a 200MHz PentiumPro running Linux) for some examples. As is seen from the group sizes, computation of the invariant subgroups is feasible even for groups for which the determination of the full subgroup lattice would be hopeless as long as the number of invariant subgroups remains small.

The column "Restriction" indicates whether restrictions to the subgroups sizes or normality were indicated to the algorithm. All the example groups are so large that computing all subgroups first and check for invariant ones afterwards would be difficult to hopeless.

6. Closing remarks

As mentioned above the algorithms described lead themselves easily to extension to the case of a nonsolvable G with solvable normal subgroup N. Extension to a nonsolvable N seems to be much more difficult and would require thorough understanding of complements in the nonsolvable case beforehand.

Parts of the work described were done during the author's work at Lehrstuhl D für Mathematik, RWTH Aachen. They form part of the author's PhD thesis written under the supervision of J. Neubüser.

The author thanks B. Eick, H. Theißen and the anonymous referees for helpful comments on prior versions of this paper.

Support by the DFG-Graduiertenkolleg "Analyse und Konstruktion in der Mathematik" at RWTH Aachen, by the DFG Schwerpunkt "Algorithmische Algebra und Zahlentheorie" and by EPSRC Grant GL/L21013 is thankfully acknowledged by the author.

References

Bosma, W., Cannon, J., Playoust, C. (1997). The magma algebra system I: The user language. *J. Symbolic Comput.*, 24(3/4):235–265.

Cannon, J., Cox, B., Holt, D. Computing the subgroup lattice of a permutation group. *Submitted*.

Cannon, J., Leedham-Green, C. R. Presentations of finite soluble groups. in preparation.

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

Eick, B. personal communication.

Eick, B. (1993). PAG-Systeme im Computeralgebrasystem GAP. Diplomarbeit, Lehrstuhl D für Mathematik, Rheinisch-Westfälische Technische Hochschule, Aachen.

Eick, B. (1997). Special presentations for finite soluble groups and computing (pre-)Frattini subgroups. In Finkelstein, L., Kantor, W. M., editors, *Groups and Computation II*, volume 28 of *DIMACS: Series in Discrete Mathematics and Theoretical Computer Science*, pages 101–112. American Mathematical Society, Providence, RI.

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

Glasby, S. P. (1989). The composition and derived lengths of a soluble group. *J. Algebra*, 120(2):406–413.

Hulpke, A. (1996). *Konstruktion transitiver Permutationsgruppen*. PhD thesis, Rheinisch-Westfälische Technische Hochschule, Aachen, Germany.

Hulpke, A. (1998). Computing normal subgroups. In Gloor, O., editor, *Proceedings of the 1998 International Symposium on Symbolic and Algebraic Computation*, pages 194–198. The Association for Computing Machinery, ACM Press.

Laue, R. (1982). Computing double coset representatives for the generation of solvable groups. In Calmet, J., editor, *EUROCAM '82*, volume 144 of *Lecture Notes in Computer Science*. Springer, Heidelberg.

Laue, R., Neubüser, J., Schoenwaelder, U. (1984). Algorithms for finite soluble groups and the SOGOS system. In Atkinson, M. D., editor, *Computational Group theory*, pages 105–135. Academic press.

Lux, K., Müller, J., Ringe, M. (1994). Peakword Condensation and Submodule Lattices: An Application of the Meat-Axe. *J. Symbolic Comput.*, 17:529–544.

Mnich, J. (1992). Untergruppenverbände und auflösbare Gruppen in GAP. Diplomarbeit, Lehrstuhl D für Mathematik, Rheinisch-Westfälische Technische Hochschule, Aachen.

Neubüser, J. (1960). Untersuchungen des Untergruppenverbandes endlicher Gruppen auf einer programmgesteuerten elektronischen Dualmaschine. *Numer. Math.*, 2:280–292.

Slattery, M. C. Computing double cosets in soluble groups. *J. Symbolic Comput.*, To appear.

Slattery, M. C. (1995). personal communication.