J. Symbolic Computation (2001) **11**, 1–000

Computing subgroups by exhibition in finite solvable groups

Bettina Eick[†] and Charles R. B. Wright[‡]

[†] *Fachbereich für Mathematik und Informatik, Universität Kassel, 34109 Kassel, Germany*
[‡] *Department of Mathematics, University of Oregon, Eugene, Oregon 97403, U.S.A.*

(Received 20 January 2000)

We present practical algorithms to compute subgroups such as Hall systems, system normalizers, $\mathfrak{F}$-normalizers and $\mathfrak{F}$-covering subgroups in finite solvable groups. An application is an algorithm to calculate head complements in finite solvable groups; that is, complements which are closely related to maximal subgroups. Our algorithms use the technique of exhibiting subgroups.

Subgroups such as Hall systems, system normalizers, $\mathfrak{F}$-normalizers and $\mathfrak{F}$-covering subgroups arise naturally in the study of finite solvable groups. Here we present practical algorithms to compute such subgroups. Besides being of interest in the theory of formations, the algorithms also yield fast methods for constructing head complements. These complements are closely related to the maximal subgroups of the underlying group and they also arise in the determination of special polycyclic generating sequences for solvable groups. Such sequences have proved to be of central importance for fast computations with finite solvable groups, and thus a practical method to obtain them has important applications.

Our approach is to start with a special type of generating set for a given solvable group and then to modify the set until it contains an easily identified generating set for the desired subgroup. This process, which is called "exhibition," was first introduced by C. R. Leedham-Green and is described in (Cannon and Leedham-Green, 1993) and (Eick, 1997). It is a powerful method for computing subgroups that are described by their intrinsic properties. One element of our approach will be a characterization of those sets of subgroups that can be simultaneously exhibited.

The paper is organized as follows. First we describe the fundamental idea of exhibiting subgroups of finite solvable groups in Section 1. Then in Section 2 we introduce the key algorithm of our paper: a method to exhibit certain normalizers in a finite solvable group. In Section 3 we show how to use such normalizers to compute head complements, and in Section 4 we describe their applications for the computation of formation theoretic subgroups. We report on the implementations of these methods in the computer algebra system GAP, see (Schönert *et al.*, 1995), and to show the practicability of our methods we give runtimes in Section 5. Finally, in Section 6 we outline a complexity analysis.

0747–7171/90/000000 + 00 $03.00/0

1. Polycyclic generating sequences and exhibition

Let G be a finite solvable group with polycyclic series $G = C_1 \rhd \ldots \rhd C_n \rhd C_{n+1} = \{1\}$. If we choose elements a_i such that $\langle a_i, C_{i+1} \rangle = C_i$, then the sequence $\mathcal{A} = (a_1, \ldots, a_n)$ is a *polycyclic generating sequence* of G. We assume throughout this paper that the polycyclic series is a composition series, so that each index $[C_i : C_{i+1}]$ is a prime, say p_i.

The tails $(a_i, \ldots, a_n)$ of $\mathcal{A}$ form polycyclic generating sequences of the subgroups C_i, and so $\mathcal{A}$ *determines* the polycyclic series. Moreover, each element of G is uniquely expressible as a *normal word* in the form $a_1^{e_1} \cdots a_n^{e_n}$ with $0 \leq e_i < p_i$ for $1 \leq i \leq n$; for short we say that $a_1^{e_1} \cdots a_n^{e_n}$ is a *normal word in* $\mathcal{A}$.

In our applications we will often choose the polycyclic series of G to refine a given normal series with elementary abelian factors. In this case we say that $\mathcal{A}$ is *compatible* with the normal series.

The polycyclic generating sequence $\mathcal{A}$ determines a power-commutator presentation of G, a type of presentation often used to represent finite solvable groups for computations; see for example (Sims, 1994) for further information. A practical algorithm to compute polycyclic generating sequences for solvable permutation groups is given in (Sims, 1990). Further, (Plesken, 1987) and (Niemeyer, 1994) present methods to obtain power-commutator presentations for finite solvable factors of finitely presented groups.

1.1. Exhibited subgroups

Let $\mathcal{A} = (a_1, \ldots, a_n)$ be a polycyclic generating sequence of G and let U be a subgroup of G. Then $\mathcal{A}$ *exhibits* U in case the subsequence of elements a_i that belong to U forms a polycyclic generating sequence of U. We denote the subsequence by $\mathcal{A} \cap U$.

It is easily seen, e.g. as a consequence of Theorem 1.4 below, that for any chain of subgroups there exists a polycyclic generating sequence simultaneously exhibiting all subgroups in the chain.

If $\mathcal{A}$ exhibits U, then $U = \langle \mathcal{A} \cap U \rangle$, but the converse is not true. For example, consider the dihedral group $G = \langle (1234), (12)(34) \rangle$, with subgroup $U = \langle (1234) \rangle$ and polycyclic generating sequence $\mathcal{A} = ((1234), (12)(34), (14)(23))$. Then $\mathcal{A} \cap U = ((1234))$, and thus $U = \langle \mathcal{A} \cap U \rangle$, but $\mathcal{A}$ does not exhibit U.

It will be useful to characterize exhibition in two ways.

Lemma 1.1. *Let U be a subgroup of G, and let $\mathcal{A} = (a_1, \ldots, a_n)$ be a polycyclic generating sequence of G that determines the composition series $G = C_1 \rhd \ldots \rhd C_n \rhd C_{n+1} = 1$ with $[C_i : C_{i+1}] = p_i$. Then the following statements are equivalent.*

(1) $\mathcal{A}$ exhibits U.
(2) U is the set of normal words in $\mathcal{A} \cap U$.
(3) $|U| = \prod_{a_i \in \mathcal{A} \cap U} p_i$.

Proof. Clearly (1) implies (2). Moreover, (2) implies (3), since the number of normal words in $\mathcal{A} \cap U$ is $\prod_{a_i \in \mathcal{A} \cap U} p_i$ and such expressions are unique. On the other hand, (3) implies (2), since U contains the set of normal words in $\mathcal{A} \cap U$ in any case and the condition in (3) implies that U cannot contain more elements.

Now suppose that (2) is true and we want to show (1). Let $\mathcal{A}_i = (a_i, \ldots, a_n)$ for $i = 1, \ldots, n+1$. First we show that $\langle \mathcal{A}_i \cap U \rangle = C_i \cap U$. Clearly, $\mathcal{A}_i \cap U \subseteq C_i \cap U$ and hence $\langle \mathcal{A}_i \cap U \rangle \leq C_i \cap U$. On the other hand, U is the set of normal words in $\mathcal{A} \cap U$ and thus $C_i \cap U$ is the set of normal words in $\mathcal{A}_i \cap U$. Therefore we obtain $C_i \cap U \leq \langle \mathcal{A}_i \cap U \rangle$.

Clearly, the subgroups $C_i \cap U$ form a subnormal chain of subgroups of U whose indices $[C_i \cap U : C_{i+1} \cap U]$ are either prime or trivial. Hence the set of subgroups $\langle \mathcal{A}_i \cap U \rangle$ contains the members of a composition series of U. Thus $\mathcal{A} \cap U$ is a polycyclic generating sequence of U. $\square$

1.2. Intersections and Products of exhibited subgroups

One of the chief advantages of the exhibition approach is the ability to immediately exhibit certain subgroups built from ones on hand.

Theorem 1.2. *Let $\mathcal{A}$ be a polycyclic generating sequence of G that simultaneously exhibits the subgroups U and V of G.*

(a) Then $\mathcal{A}$ exhibits $U \cap V$.
(b) If $UV = VU$, then $\mathcal{A}$ exhibits $\langle U, V \rangle$.

Proof. (a) By Lemma 1.1, $U \cap V$ is the set of elements that are normal words in both $\mathcal{A} \cap U$ and $\mathcal{A} \cap V$. Since representations as normal words are unique, these are the elements that are normal words in $\mathcal{A} \cap (U \cap V)$. By Lemma 1.1 again, $\mathcal{A}$ exhibits $U \cap V$.

(b) Using (a) and applying Lemma 1.1 to U, V, $U \cap V$ and finally to UV we obtain

$$\begin{aligned} |UV| &= |U||V|/|U \cap V| \\ &= \prod_{a_i \in \mathcal{A} \cap U} p_i \prod_{a_i \in \mathcal{A} \cap V} p_i \bigg/ \prod_{a_i \in \mathcal{A} \cap (U \cap V)} p_i \\ &= \prod_{a_i \in (\mathcal{A} \cap U) \cup (\mathcal{A} \cap V)} p_i \leq \prod_{a_i \in \mathcal{A} \cap UV} p_i \leq |UV|. \end{aligned}$$

Hence we have equality and the desired result is obtained. $\square$

If we have exhibited a set of subgroups, then by Theorem 1.2 their intersections and permuting products can be obtained without further computational effort. For example, suppose that we want to exhibit a Hall system of G, i.e., a set of permuting Hall subgroups, one for each set of primes dividing the order of G. By Theorem 1.2 it is enough to exhibit either all Sylow subgroups in the Hall system (a Sylow basis) or all Sylow complements in the Hall system (a complement basis), since we can derive all the other Hall subgroups as products from the Sylow basis or as intersections from the complement basis.

The ability to compute intersections and certain products quickly will be important when we compute system normalizers and related subgroups in what follows. Theorem 1.2 also yields the following facts that we will use later.

Proposition 1.3. *Let $\mathcal{A}$ be a polycyclic generating sequence for G. If $\mathcal{A}$ exhibits the π-Hall subgroup H of G and also the subgroup U of G, then $H \cap U$ is a π-Hall subgroup of U. Hence if $\mathcal{A}$ exhibits the Hall system Σ for G, then Σ reduces into every subgroup of G that $\mathcal{A}$ exhibits.*

PROOF. By Theorem 1.2, $\mathcal{A}$ exhibits $H \cap U$. Thus the result follows with Lemma 1.1. $\square$

1.3. A characterization of the sets of subgroups that can be exhibited

It is in general not possible to exhibit simultaneously all members of a given set of subgroups. The following theorem characterizes in a natural and useful way those sets of subgroups for which there exists a polycyclic generating sequence simultaneously exhibiting all subgroups in the set.

THEOREM 1.4. *Let G be a finite solvable group and let X be a set of subgroups of G. Then there exists a polycyclic generating sequence of G exhibiting all subgroups in X if, and only if, there exists a composition series $G = C_1 \rhd \ldots \rhd C_{n+1} = \{1\}$ such that for each $i \in \{1, \ldots, n\}$ the factor C_i/C_{i+1} is covered by the intersection V_i of all those members of X that cover C_i/C_{i+1}.*

In this case we can choose $a_i \in V_i \cap C_i \setminus C_{i+1}$ to obtain a polycyclic generating sequence $\mathcal{A} = (a_1, \ldots, a_n)$ that exhibits X and the series $G = C_1 \rhd \ldots \rhd C_{n+1} = \{1\}$.

PROOF. Suppose first that $\mathcal{A} = (a_1, \ldots, a_n)$ is a polycyclic generating sequence of G that exhibits all subgroups in X. Let $G = C_1 \rhd \ldots \rhd C_{n+1} = 1$ be the composition series determined by $\mathcal{A}$, and consider $i \in \{1, \ldots, n\}$. Suppose that U in X covers C_i/C_{i+1}. Since U is exhibited by $\mathcal{A}$, we have $a_i \in U$. Thus a_i is an element of the intersection V_i, and hence V_i covers C_i/C_{i+1} as well.

Suppose now that there exists a composition series $G = C_1 \rhd \ldots \rhd C_{n+1} = 1$ of G such that for each $i \in \{1, \ldots, n\}$ the intersection V_i of the members of X covering C_i/C_{i+1} also covers C_i/C_{i+1}. (Here $V_i = G$ if no member of X covers C_i/C_{i+1}.) For each i we choose $a_i \in V_i \cap (C_i \setminus C_{i+1})$ and use inverse induction on i to show that $\mathcal{A} = (a_1, \ldots, a_n)$ exhibits all subgroups in X. Let $U \in \mathsf{X}$ and suppose for induction that $U \cap C_{i+1}$ is exhibited by $\mathcal{A}$. If U avoids C_i/C_{i+1}, then $U \cap C_i = U \cap C_{i+1}$ and thus $U \cap C_i$ is exhibited as well. If U covers C_i/C_{i+1}, then $a_i \in V_i \leq U$ and thus a_i together with $\mathcal{A} \cap (U \cap C_{i+1})$ yields a subsequence of $\mathcal{A}$ that is a polycyclic generating sequence of $U \cap C_i$. Thus $\mathcal{A}$ exhibits $U \cap C_i$ in this case too. $\square$

Theorem 1.4 provides a proof that every chain of subgroups can be exhibited, since the intersection of subgroups in such a chain is again a subgroup in the chain. The condition of Theorem 1.4 is also trivially fulfilled if a set X of subgroups has the property that each composition factor is covered by at most one member of X; for example, every set of Sylow subgroups for different primes can be exhibited and thus, by Theorem 1.2, every Hall system can be.

To prove that a certain set of subgroups can be exhibited it is sometimes more natural or more useful to consider a subnormal series that is not necessarily a composition series of G. It is an easy consequence of Theorem 1.4 to obtain the following similar characterization using a subnormal series instead.

COROLLARY 1.5. *Let G be a finite solvable group and X a set of subgroups of G. Then there exists a polycyclic generating sequence of G exhibiting all members of X if, and only if, there exists a subnormal series $G = S_1 \rhd \ldots \rhd S_m \rhd S_{m+1} = \{1\}$ such that for each $j \in \{1, \ldots, m\}$*

(a) each subgroup in X *either covers or avoids* S_j/S_{j+1}*, and*
(b) the intersection W_j *of all those members of* X *that cover* S_j/S_{j+1} *also covers* S_j/S_{j+1}*.*

PROOF. If there exists a polycyclic generating sequence $\mathcal{A}$ of G exhibiting X, then we may choose the composition series determined by $\mathcal{A}$ as subnormal series and invoke Theorem 1.4.

Now suppose that we are given a subnormal series and an X that satisfy (a) and (b). Refine the series to a composition series $G = C_1 \triangleright \ldots \triangleright C_{n+1} = 1$, and consider the chain $S_j \geq C_i > C_{i+1} \geq S_{j+1}$. Since each subgroup in X either covers or avoids S_j/S_{j+1}, the subgroups in X covering C_i/C_{i+1} are exactly the subgroups in X covering S_j/S_{j+1}. By assumption, the intersection of these subgroups covers S_j/S_{j+1}, and thus it covers C_i/C_{i+1}. Hence X is exhibited, by Theorem 1.4. $\square$

It is not always possible to exhibit a complete set of representatives of the conjugacy classes of maximal subgroups of a group; such a goal is unattainable even for elementary abelian groups. The head complements introduced by Leedham-Green and described in (Cannon and Leedham-Green, 1993) and (Eick, 1997) provide a useful substitute, however, and in Section 3 below we give an algorithm to exhibit head complements. In Section 4 we describe algorithms that exhibit system normalizers and subgroups associated with the theory of formations, together with their corresponding Hall systems.

1.4. Hall generating sequences

An important application of Theorem 1.4 for our purposes is included in the following obvious consequence of Corollary 1.5.

COROLLARY 1.6. *Let* G *be a finite solvable group and let* $G = K_1 \triangleright \ldots \triangleright K_{m+1} = \{1\}$ *be a normal series of* G *with elementary abelian factors. Furthermore let* Σ *be a Hall system of* G*. Then there exists a polycyclic generating sequence* $\mathcal{A}$ *of* G *compatible with the normal series and exhibiting the Hall system* Σ*.*

We call such a polycyclic generating sequence $\mathcal{A}$ as described in Corollary 1.6 a *Hall generating sequence*. These sequences will be the starting points for all of our computations. In Appendix A we give an algorithm that starts with a normal series with elementary abelian factors and computes a polycyclic generating sequence that is compatible with the normal series and that exhibits a Hall system. Another algorithm for computing a Hall generating sequence is described in (Cannon and Leedham-Green, 1993).

2. Computing certain normalizers

In this section we introduce an algorithm to exhibit subgroups of the form $N_G(S_{p'} \cap M)$, where $S_{p'}$ is a p-complement and M a normal subgroup of G. Such subgroups will play key roles in the algorithms in later sections.

Methods are known to compute the normalizer of an arbitrary subgroup of a finite solvable group; for example, a practical algorithm is described in (Celler *et al.*, 1990). While our method is restricted to subgroups of a specific type, in that setting it is more efficient than the other known methods for this purpose. Moreover, our algorithm yields not just a generating set for the normalizer, but even a polycyclic generating sequence of G that exhibits the normalizer.

We emphasize that our approach allows us to avoid the computation of chief factors, which is a standard approach in theoretical work with finite solvable groups. From an algorithmic point of view, our indifference to whether factors are chief yields a significant speedup in performance, since a chief series would generally take longer to obtain than our series, and furthermore would typically entail more steps down an elementary abelian series in any algorithm based on the homomorphism principle.

2.1. Exhibiting $N_G(S_{p'} \cap M)$

Let p be a prime and M a normal subgroup of G. As setup for our algorithm we use a normal series $\mathcal{K} = (G = K_1 \rhd K_2 \rhd \ldots \rhd K_m \rhd K_{m+1} = \{1\})$ with elementary abelian factors such that each p-factor is either M-central or M-hypereccentric, i.e. contains no M-central G-chief factor. In Section 2.2 we describe a method to obtain such a series $\mathcal{K}$.

Let $\mathcal{A}$ be a Hall generating sequence associated to $\mathcal{K}$; that is, the composition series determined by $\mathcal{A}$ refines the series $\mathcal{K}$, and $\mathcal{A}$ exhibits a Hall system $\Sigma = \{S_\pi \mid \pi \text{ a set of primes}\}$ of G. We want to modify $\mathcal{A}$ to a polycyclic generating sequence which additionally exhibits $N_G(S_{p'} \cap M)$, where $S_{p'}$ is the p-complement in Σ.

Theorem V.1(1.5) of (Doerk and Hawkes, 1992), with $\pi = \{p\}$ and $\nu(p) = M$, says that $N_G(S_{p'} \cap M)$ either covers or avoids each chief factor of G, and covers a p-chief factor precisely if $S_{p'} \cap M$ centralizes it. Since $S_{p'} \cap M$ centralizes a chief factor if, and only if, M acts on it as a p-group, since $M \trianglelefteq G$, and since $N_G(S_{p'} \cap M)$ covers all p'-chief factors, it follows that $N_G(S_{p'} \cap M)$ avoids the M-hypereccentric p-chief factors of G and covers all other chief factors. Thus $N_G(S_{p'} \cap M)$ either covers or avoids each factor in $\mathcal{K}$. By Corollary 1.5, G has a polycyclic generating sequence that simultaneously exhibits Σ, the subgroups in $\mathcal{K}$ and the subgroup $N_G(S_{p'} \cap M)$.

We wish to modify $\mathcal{A}$ by working down the factors of the series $\mathcal{K}$, using the following fact.

Lemma 2.1. *Let H be a π-Hall subgroup and M a normal subgroup of the finite solvable group G. Then $N_G(H \cap M)K/K = N_{G/K}(HK/K \cap MK/K)$ for every normal subgroup K of G.*

Proof. Since HK/K is a π-Hall subgroup in G/K, it follows that $HK/K \cap MK/K$ is a π-Hall subgroup in MK/K, as is $(H \cap M)K/K$. Thus $HK \cap MK = (H \cap M)K$.

We may assume that K is minimal normal in G. If K is a π'-group, then $H \cap M$ is a π-Hall subgroup in $(H \cap M)K$, so by the Frattini argument $N_G((H \cap M)K) = N_G(H \cap M)K$. If K is a π-group, then $K \le H$, so $N_G((H \cap M)K) = N_G(H \cap MK) \le N_G(H \cap MK \cap M) = N_G(H \cap M) \le N_G((H \cap M)K)$. $\square$

Clearly, our setup is inherited by the factor groups G/K_i; in fact, the induced sequences $\mathcal{A}/K_i = (a_1K_i, \ldots, a_{j_i}K_i)$ form Hall generating sequences of G/K_i associated with the normal series $K_1/K_i \rhd \ldots \rhd K_i/K_i$ and with the Hall systems $\{S_\pi K_i/K_i\}$, where the index j_i is chosen such that $(a_{j_i+1}, \ldots, a_n)$ forms a polycyclic generating sequence of K_i. Hence we may assume by induction that $\mathcal{A}/K_m$ exhibits $N_{G/K_m}(S_{p'}K_m/K_m \cap MK_m/K_m)$, which is equal to $N_G(S_{p'} \cap M)K_m/K_m$, according to Lemma 2.1. Therefore it will be enough to show that if $\mathcal{A}$ exhibits $N_G(S_{p'} \cap M)K_m$, then $\mathcal{A}$ can be modified to exhibit $N_G(S_{p'} \cap M)$ in addition to $\mathcal{K}$ and Σ.

Let $K = K_m$, and suppose that K is a q-group for the prime q. If $q \neq p$ or if $q = p$ and K is M-central, then $K \leq N_G(S_{p'} \cap M)$, and thus $\mathcal{A}$ exhibits $N_G(S_{p'} \cap M)$ by induction.

Thus we assume now that K is an M-hypereccentric p-subgroup of G, so $N_G(S_{p'} \cap M)$ avoids K, and thus $N_G(S_{p'} \cap M)$ is a complement to K in $N_G(S_{p'} \cap M)K$. By assumption, $\mathcal{A}$ exhibits $N_G(S_{p'} \cap M)K$; say the subsequence $(a_{i_1}, \ldots, a_{i_r}, a_{l+1}, \ldots, a_n)$ is a polycyclic generating sequence of this subgroup, where $(a_{l+1}, \ldots, a_n)$ is a polycyclic generating sequence of K. Then each complement to K has a polycyclic generating sequence of the form $(a_{i_1}k_{i_1}, \ldots, a_{i_r}k_{i_r})$ for certain elements $k_{i_j} \in K$. Our aim is to compute elements $k_{i_1}, \ldots, k_{i_r}$ corresponding to the complement $N_G(S_{p'} \cap M)$.

Since $\mathcal{A}$ exhibits Σ, each element in $\mathcal{A}$ is either contained in $S_{p'}$ or in the exhibited Sylow subgroup S_p. If a_{i_j} is an element of $S_{p'}$, then $a_{i_j} \in N_G(S_{p'} \cap M)$, and we may choose $k_{i_j} = 1$.

Now consider the case $a_{i_j} \in S_p$. To simplify notation we will write $a = a_{i_j}$. Since $a \in N_G(S_{p'} \cap M)K$, we have $[m, a] \in (S_{p'} \cap M)K$ for each m in $S_{p'} \cap M$. Thus we can factor the commutator into

$$[m, a] = l_m \cdot h_m \quad \text{with} \quad l_m \in S_{p'} \cap M \quad \text{and} \quad h_m \in K$$

and since $K \cap S_{p'} \cap M = \{1\}$ this factorization is unique. Hence for k in K with ak in $N_G(S_{p'} \cap M)$ we get

$$\begin{aligned} [m, ak] &= [m, a] \cdot [m^a, k] \\ &= l_m \cdot h_m \cdot [m^a, k] \\ &= l_m \cdot x_m \quad \text{with} \quad x_m = h_m \cdot [m^a, k] \in K. \end{aligned}$$

Again, this factorization of $[m, ak]$ into elements l_m in $S_{p'} \cap M$ and x_m in K is unique. Now $ak \in N_G(S_{p'} \cap M)$ if, and only if, $[m, ak] \in S_{p'} \cap M$ for every m in $S_{p'} \cap M$, i.e., if, and only if, $x_m = 1$ and

$$h_m = [m^a, k]^{-1} = [k, m^a]$$

for each m in $S_{p'} \cap M$.

The set of elements m in $S_{p'} \cap M$ for which $[m, ak] \in S_{p'} \cap M$ is a group, so if $\{m_1, \ldots, m_s\}$ is a generating set of $S_{p'} \cap M$ then

$$\begin{aligned} ak \in N_G(S_{p'} \cap M) \quad &\Leftrightarrow \quad [m_i, ak] = l_{m_i} \quad \text{for} \quad 1 \leq i \leq s \\ &\Leftrightarrow \quad h_{m_i} = [k, m_i^a] \quad \text{for} \quad 1 \leq i \leq s. \end{aligned}$$

Thus if the element $a = a_{i_j}$ and a generating set of $S_{p'} \cap M$ are given, then we can compute k_{i_j} as a solution of the system of s inhomogeneous equations $h_{m_i} = [k, m_i^a]$. Note that h_{m_i} is straightforward to obtain; since K is exhibited by $\mathcal{A}$, it is just the K-part of the exponent vector of $[m_i, a]$ with respect to $\mathcal{A}$. Furthermore, since K is an elementary abelian p-group, the equations for k can be translated into a system of inhomogeneous linear equations over the field $\mathbb{F}_p$.

Now we modify the given Hall generating sequence $\mathcal{A}$ by substituting $a_{i_j}k_{i_j}$ for a_{i_j}. The resulting polycyclic generating sequence $\mathcal{B}$ is obviously still compatible with the series $\mathcal{K}$. Furthermore, since the only elements of $\mathcal{A}$ that we modify are in the Sylow subgroup S_p, and since $K \leq S_p$, the resulting polycyclic generating sequence $\mathcal{B}$ exhibits Σ. Thus $\mathcal{B}$ is a Hall generating sequence associated to $\mathcal{K}$ and Σ that in addition exhibits $N_G(S_{p'} \cap M)$.

2.2. Separating M-central and M-hypereccentric factors

It remains to show how to construct a normal series $\mathcal{K}$ as required in the setup of Section 2.1. Suppose that $L_1, \ldots, L_t$ is an arbitrary normal series with elementary abelian factors of G. We refine this series such that each p-factor is either M-central or M-hypereccentric.

Let $L = L_i/L_{i+1}$ be a p-factor in the given series. Clearly, $[L, M]$ is normal in G/L_{i+1} and $L/[L, M]$ is M-central. We calculate iterated commutators until the series $L, [L, M], [[L, M], M], \ldots$ becomes stable at a normal subgroup U of L with $[U, M] = U$.

If $U = 1$, then we have constructed a G-normal series for L with M-central factors. Suppose that U is non-trivial. Consider a G-normal series $M = M_1 \rhd M_2 \rhd \ldots \rhd M_d \rhd M_{d+1} = \{1\}$ with nilpotent factor groups. Such a series may be obtained by computing commutators or by using the given elementary abelian G-normal series compatible with the Hall generating sequence $\mathcal{A}$. Since $[U, M] = U$ and $[U, 1] = 1$, there exists a smallest index i such that $[U, M_i] < U$. Clearly, $[U, M_i]$ is normal in G/L_{i+1}. We use the following observation to show that $U/[U, M_i]$ is M-hypereccentric.

Lemma 2.2. *If the nilpotent group N acts on the abelian group A with $[A, N] = A$, then A is hypereccentric under the action of N.*

Proof. Consider the split extension H of A by N. The nilpotent residual subgroup $H^{\mathfrak{N}}$ of H is contained in A, since H/A is nilpotent. On the other hand $[A, N] = A$; thus $A = H^{\mathfrak{N}}$. Since A is abelian, by Theorem 5.15 in (Carter and Hawkes, 1967) each complement to A in H is a system normalizer of H. Thus N is a system normalizer of H. By Theorem I(5.6) of (Doerk and Hawkes, 1992) a system normalizer avoids exactly the non-central chief factors, so each chief factor in A must be non-central. Therefore A is H-hypereccentric and thus N-hypereccentric. $\square$

By definition and Lemma 2.2, the factor $U/[U, M_i]$ is hypereccentric under the action of the nilpotent group M_{i-1}/M_i. Therefore $U/[U, M_i]$ is also M-hypereccentric.

The first factor L/U in the chain $L \trianglerighteq U \trianglerighteq [U, M_i]$ is M-hypercentral, and the second is M-hypereccentric. If $[U, M_i] \neq 1$, then we may iterate the whole procedure, starting with $[U, M_i]$ in place of L, until we arrive at the trivial subgroup of L. Thus we obtain a refinement of the factor L_i/L_{i+1} in the desired form.

3. Computing head complements

In the following lemma we observe that the algorithm to exhibit normalizers of the form $N_G(S_{p'} \cap M)$ can be applied to compute conjugacy classes of complements in certain situations.

Lemma 3.1. *Let A be an abelian normal p-subgroup of the finite group G, and let M be a normal subgroup of G such that M/A is nilpotent and $[A, M] = A$. Then there is exactly one conjugacy class of complements to A in G, namely the set of subgroups of form $N_G(S_{p'} \cap M)$, for $S_{p'}$ a p-complement of G.*

PROOF. Let $Q = S_{p'} \cap M$. Then Q is a p-complement of M and, since M/A is nilpotent, QA is a normal subgroup of G. By the Frattini argument, $G = AN_G(Q)$. Since A is abelian, $N_A(Q) = C_A(Q) = C_A(M)$, so $N_A(Q) = 1$ by Lemma 2.2, since $[A, M] = A$. Hence the conjugates of $N_G(Q)$ complement A in G. On the other hand, if X complements A in G, then $M \cap X$ complements A in M, so $M \cap X$ must be a p-complement of M. Since $X \leq N_G(M \cap X)$, and since $N_G(M \cap X)$ complements A, we have $X = N_G(M \cap X)$. □

Head complements are associated with the so-called *special* polycyclic generating sequences. We include a brief introduction to these sequences here.

Let $G = G_1 \rhd \ldots \rhd G_l \rhd \{1\}$ be the lower nilpotent series of G, and let G_i^*/G_{i+1} be the Frattini subgroup of G_i/G_{i+1}. Then the so-called LG-series is an elementary abelian normal series which refines the series $G = G_1 \rhd G_1^* \trianglerighteq G_2 \rhd \ldots \rhd G_l \trianglerighteq G_l^* \trianglerighteq \{1\}$. The factors G_i/G_i^* are called the *heads* of G. A *special polycyclic generating sequence* is a Hall generating sequence compatible with the LG-series and exhibiting a complement to each head of G.

An effective algorithm to compute a Hall generating sequence compatible with the LG-series in a finite solvable group is introduced in (Cannon and Leedham-Green, 1993). Hence we may assume that we are given such a generating sequence $\mathcal{A}$ for G. We want to exhibit a complement to the head $H = G_i/G_i^*$ with $i > 1$. Since H is a direct product of elementary abelian groups, we can write $H = H_p \times H_{p'}$ for a prime p. Let $A = H/H_{p'} \cong H_p$, an elementary abelian p-factor group of H. Let $M = G_{i-1}/G_i^*$. Since G_{i-1}/G_i is a maximal nilpotent factor of G_{i-1}, we have that $[A, M] = A$. Thus the hypotheses of Lemma 3.1 are fulfilled and we can use this lemma and the method of Section 2 to exhibit a complement to A in G.

Now we iterate this procedure with the other primes p dividing the order of the head H to exhibit a complement to the head. For each step up the normal series we have to multiply elements of $\mathcal{A} \setminus G_i$ by preimages of elements of $H/H_{p'}$. Clearly, we can choose these preimages as preimages of elements of H_p, so the steps for the various primes p dividing the order of H do not interfere with each other. Thus we can modify $\mathcal{A}$ such that it exhibits a complement to each factor $H/H_{p'}$, and thus exhibits also the intersection of these complements, which is a complement to H.

This modification of the polycyclic generating sequence will not affect its compatibility with the LG-series or with the Hall system. Moreover, if we change $\mathcal{A}$ by multiplying its entries by elements of G_{i+1}, then it will still exhibit the complement to G_i/G_i^*. Thus by working down the lower nilpotent series we can construct a Hall generating sequence that exhibits a complement to every head, i.e., a special polycyclic generating sequence.

For an alternative proof that it is possible to exhibit a Hall system and complements to all heads simultaneously, see (Eick, 1997).

4. Computing formation theoretic subgroups

This section contains algorithms to compute formation theoretic subgroups of finite solvable groups. For definitions and background on this subject we refer to (Gaschütz, 1963), (Carter and Hawkes, 1967) and (Doerk and Hawkes, 1992).

Let $\mathfrak{F}$ be a formation locally defined by the set $\{\mathfrak{F}_p \mid p \text{ prime}\}$ of formations. To avoid technical problems, we assume that the local definition is integrated, i.e., that $\mathfrak{F}_p \subseteq \mathfrak{F}$ for each p. We allow $\mathfrak{F}_p$ to be the empty set, and we call the set of primes p such that $\mathfrak{F}_p$ is nonempty the *support* of $\mathfrak{F}$. Associated to each formation $\mathfrak{F}$ and each group G is the

$\mathfrak{F}$-*residual* subgroup $G^{\mathfrak{F}}$ of G, the smallest normal subgroup of G whose factor group is in $\mathfrak{F}$.

Two types of subgroups of interest in connection with locally defined formations $\mathfrak{F}$ are the $\mathfrak{F}$-normalizers and $\mathfrak{F}$-covering subgroups of finite solvable groups. Both of these types of subgroups form characteristic conjugacy classes that are invariant under taking homomorphic images. Furthermore, these subgroups are themselves in the formation $\mathfrak{F}$. Well known examples of such subgroups are system normalizers and Carter subgroups, which arise as $\mathfrak{F}$-normalizers and $\mathfrak{F}$-covering subgroups for the formation $\mathfrak{F}$ of nilpotent groups.

In this section we will describe efficient algorithms to compute $\mathfrak{F}$-normalizers, $\mathfrak{F}$-covering subgroups and $\mathfrak{F}$-residuals for locally defined formations $\mathfrak{F}$ and finite solvable groups G. For this purpose we represent the locally defined formation $\mathfrak{F}$ by a function that computes for each prime p in the support of $\mathfrak{F}$ the $\mathfrak{F}_p$-residual $G^{\mathfrak{F}_p}$ of G and, when necessary, residual subgroups $U^{\mathfrak{F}_p}$ for subgroups U of G. Each of our algorithms takes as input a Hall generating sequence and a means of computing the needed residuals.

4.1. Computing $\mathfrak{F}$-normalizers

To describe the $\mathfrak{F}$-normalizer algorithm we consider a slightly more general context. Let G be a finite solvable group, and let σ be a set of primes. For each prime p in σ let M_p be a normal subgroup of G, and define the function ν from σ into the set of normal subgroups of G by $\nu\colon p \mapsto M_p$. A ν-*normalizer* of G is a subgroup

$$D_\nu(G,\Sigma) = S_\sigma \cap \bigcap_{p\in\sigma} N_G(S_{p'} \cap M_p)$$

where Σ is a Hall system with σ-Hall subgroup S_σ and p-complements $S_{p'}$. If the normal subgroup M_p is chosen to be the residual $G^{\mathfrak{F}_p}$ for each prime p in σ, then the resulting ν-normalizer

$$D_{\mathfrak{F}}(G,\Sigma) = S_\sigma \cap \bigcap_{p\in\sigma} N_G(S_{p'} \cap G^{\mathfrak{F}_p})$$

is called an $\mathfrak{F}$-*normalizer* of G. Thus $\mathfrak{F}$-normalizers are a special case of ν-normalizers.

We can compute ν-normalizers of G by exhibition. Suppose that we are given a Hall generating sequence $\mathcal{A}$ of G that is compatible with an elementary abelian normal series $G = K_1 \triangleright K_2 \triangleright \ldots \triangleright K_m \triangleright K_{m+1} = \{1\}$ and that exhibits the Hall system Σ. By the results of Section 2.2, we may suppose that each factor K_i/K_{i+1} of p-power order is either M_p-central or M_p-hypereccentric for each p in σ. To obtain a polycyclic generating sequence that exhibits $D_\nu(G,\Sigma)$ as well, we modify $\mathcal{A}$ so that for each p in σ it exhibits the subgroup $N_G(S_{p'} \cap M_p)$, using the algorithm described in Section 2. Since this algorithm only modifies p-elements by p-elements, we can use it to exhibit all of the normalizers $N_G(S_{p'} \cap M_p)$ simultaneously. Moreover Σ remains exhibited throughout this process. Once all subgroups $N_G(S_{p'} \cap M_p)$ are exhibited, the intersection $D_\nu(G,\Sigma)$ is exhibited as well, by Theorem 1.2.

4.2. Computing $\mathfrak{F}$-covering subgroups

As above, let G be a finite solvable group and let $\mathfrak{F}$ be a locally defined formation. An $\mathfrak{F}$-*covering* subgroup of G is a subgroup U such that $U \in \mathfrak{F}$ and $UV^{\mathfrak{F}} = V$ for all subgroups V with $U \leq V \leq G$. Our method for computing such subgroups is based on the following facts ((Gaschütz, 1963) Hilfssatz 2.3 and (Carter and Hawkes, 1967) Theorem 5.6, or (Doerk and Hawkes, 1992) Proposition III(3.7) and Theorem V(4.2)).

PROPOSITION 4.1. *Let $\mathfrak{F}$ be a locally defined formation and G a finite solvable group.*

(a) Let $K \trianglelefteq G$ and $U \leq G$ such that U/K is an $\mathfrak{F}$-covering subgroup of G/K. If V is an $\mathfrak{F}$-covering subgroup of U, then V is also an $\mathfrak{F}$-covering subgroup of G.
(b) If K is a nilpotent normal subgroup of U with $U/K \in \mathfrak{F}$, then the $\mathfrak{F}$-normalizers of U coincide with the F-covering subgroups of U.

Let $\mathcal{A}$ be a Hall generating sequence that exhibits a Hall system Σ and that is compatible with a series $G = K_1 \triangleright \ldots \triangleright K_m \triangleright K_{m+1} = \{1\}$ of normal subgroups whose factors are p-groups. For example, we can use an elementary abelian normal series, or, in case $\mathcal{A}$ is a special polycyclic generating sequence, we may refine the lower nilpotent series by taking its maximal p-factors. Suppose inductively that $\mathcal{A}$ exhibits a subgroup U such that U/K_j is an $\mathfrak{F}$-covering subgroup of G/K_j. We wish to exhibit an $\mathfrak{F}$-normalizer of U/K_{j+1}, which by Proposition 4.1 will be $\mathfrak{F}$-covering in G/K_{j+1}. To do this it will be enough to consider the case that $K_{j+1} = 1$. Let $K = K_j$, and suppose that K is a p-group.

If p is not in the support σ of $\mathfrak{F}$, then $S_{p'} \cap U$ is an $\mathfrak{F}$-covering subgroup of U. Since $\mathcal{A}$ already exhibits this subgroup, by Theorem 1.2, no change in $\mathcal{A}$ is required.

Now suppose that $p \in \sigma$. By Proposition 1.3, $\Sigma \cap U$ is a Hall system of U. We wish to modify $\mathcal{A}$ to exhibit the corresponding $\mathfrak{F}$-normalizer

$$D_{\mathfrak{F}}(U, \Sigma \cap U) = S_\sigma \cap N_U(S_{p'} \cap U^{\mathfrak{F}_p}) \cap \bigcap_{p \neq q \in \sigma} N_U(S_{q'} \cap U^{\mathfrak{F}_q}).$$

Now $U/K \in \mathfrak{F}$ and $D_{\mathfrak{F}}(U, \Sigma \cap U)$ is an $\mathfrak{F}$-covering subgroup of U, so $U = KD_{\mathfrak{F}}(U, \Sigma \cap U)$. For $p \neq q \in \sigma$ we have $K \leq S_{q'}$, and hence $K \leq N_U(S_{q'} \cap U^{\mathfrak{F}_q})$. Since we have $D_{\mathfrak{F}}(U, \Sigma \cap U) \subseteq N_U(S_{q'} \cap U^{\mathfrak{F}_q})$ as well, and since $U = KD_{\mathfrak{F}}(U, \Sigma \cap U)$, it follows that $U = S_\sigma \cap \bigcap_{p \neq q \in \sigma} N_U(S_{q'} \cap U^{\mathfrak{F}_q})$, and thus $D_{\mathfrak{F}}(U, \Sigma \cap U) = N_U(S_{p'} \cap U^{\mathfrak{F}_p})$, a single normalizer of the type discussed in Section 2. Since $D_{\mathfrak{F}}(U, \Sigma \cap U)$ covers U/K, we only need to employ the homomorphism principle to loop downward over an elementary abelian U-normal series through K in which all factors are either $U^{\mathfrak{F}_p}$-central or $U^{\mathfrak{F}_p}$-hypereccentric.

4.3. COMPUTING $\mathfrak{F}$-RESIDUALS

Practical methods are known that compute residual subgroups for a number of important locally induced formations, based on their special properties. A generic approach is possible that proceeds from the group G downwards until no more $\mathfrak{F}$-central factors can be found, but for practical computation in the general case we prefer a method based on the following fact (cf. Theorem IV(3.2) of (Doerk and Hawkes, 1992)).

PROPOSITION 4.2. *Let G be a finite solvable group and $\mathfrak{F}$ a locally defined formation with support σ. Then*

$$G^{\mathfrak{F}} = O^\sigma(G) \prod_{p \in \sigma} O^{pp'}(G^{\mathfrak{F}_p}).$$

Given the groups $G^{\mathfrak{F}_p}$ for all primes p in σ, this method only requires computing normal closures. It also obviously generalizes to deal with "internal formations" of the sort considered in (Wright, 1973a) and (Wright, 1973b).

5. Implementation and practicality

We have implemented our algorithms in the computer algebra system GAP 3.4 (see (Schönert *et al.*, 1995)). This section contains some timings of our implementations, using the following groups as examples.

- $MFi22$ is a maximal subgroup of order $2^8 \cdot 3^9$ of the finite simple group Fi_{22}.
- $U \wr C_3$ is a wreath product of the subgroup U of upper triangular matrices in $GL(4,7)$ with the cyclic group of order 3. This group has order $2^{12} \cdot 3^{13} \cdot 7^{18}$.
- Lux is a group of order $2^{55} \cdot 3^7 \cdot 7^3$. It was constructed so that a chief series would be hard to compute.
- $Dark$ is a group of order $2^3 \cdot 3^9 \cdot 5^{24} \cdot 7 \cdot 31^8$. See (Doerk and Hawkes, 1992), pp. 630ff, for an outline of its construction.

All of our algorithms depend on having a Hall generating sequence as starting point. The GAP 3 command `SpecialAgGroup(G, "noHead")` provides such sequences. The sample timings below do not include this preprocessing step. To give the reader an idea of the practicality of our methods, we present the times to exhibit a set of head complements, an $\mathfrak{F}$-normalizer and an $\mathfrak{F}$-covering subgroup for the formation $\mathfrak{F}$ of supersolvable groups. We chose to describe experiments with this formation because its local definition is moderately hard to compute with.

The timings in the following table were obtained using GAP 3.4.4 started with 8 megabytes of workspace on a 486 PC. They include garbage collections, and thus reflect on the space requirements of the algorithms as well. Times are given in seconds.

	head complements		$\mathfrak{F}$-normalizer		$\mathfrak{F}$-covering subgroup	
group	number	time	order	time	order	time
$MFi22$	4	0.1	$2^2 \cdot 3^3$	0.3	$2^2 \cdot 3^9$	2.1
$U \wr C_3$	3	0.6	$2^4 \cdot 3^{13}$	1.1	$2^4 \cdot 3^{13}$	0.8
Lux	4	1.8	$2 \cdot 3^7 \cdot 7$	6.0	$2 \cdot 3^7 \cdot 7$	6.3
$Dark$	6	1.0	$3^2 \cdot 7$	0.9	$3^3 \cdot 7 \cdot 31^2$	10.0

The comparatively large time for the $\mathfrak{F}$-covering subgroup of the group $Dark$ comes from the computation of the local residuals, which is rather complicated in this case. Altogether the timings are at most 10 seconds, although some of the groups considered are already quite large.

6. Complexity analysis

We measure the algorithms' computational effort by the total number of group multiplications, field multiplications and field additions they entail. The input parameters are the length n of the input polycyclic generating sequence for the group G, the size p of the largest prime divisor of $|G|$, and a parameter t describing the complexity of an algorithm to compute the residual subgroups $U^{\mathfrak{F}_q}$ for $U \le G$ and q a prime.

Field operations are used in the normalizer calculation, where the modification of a single generator takes $O(n^4)$ field operations in addition to $O(n^3 \log p)$ group operations. The remaining algorithms use group multiplications only.

We need a few well-known algorithms to compute with groups given by polycyclic generating sequences; see (Laue *et al.*, 1984) for more information on such methods. The basic steps of computing the exponent vector for an element relative to a polycyclic generating sequence and of finding an induced polycyclic generating sequence for a subgroup require $O(n \log p)$ and $O((r+n^2)n \log p)$ operations, respectively, where r is the number of generators of the subgroup in question.

The most time-consuming step in computing $\mathfrak{F}$-residual subgroups is finding normal closures, which can be done in $O(n^4 \log p)$ operations. Thus finding a locally defined residual subgroup has complexity $O(nt + n^5 \log p)$, with t typically negligible.

The first step in the $\mathfrak{F}$-normalizer calculation is the refinement of the elementary abelian series exhibited by a given Hall generating sequence as described in Section 2.2. This takes $O(n^4 \log p \log n)$ operations. To modify a single element of a polycyclic generating sequence as required by the $\mathfrak{F}$-normalizer algorithm takes $O(n^3(\log p + n))$ operations, so the complete $\mathfrak{F}$-normalizer algorithm runs in time $O(n(t + n^4 \log p))$. Hence finding an $\mathfrak{F}$-covering subgroup takes $O(n^2(t + n^4 \log p))$ operations.

Appendix A. Computing a Sylow complement system

This appendix contains an algorithm to construct a polycyclic generating sequence that exhibits a system of Sylow complements of a finite solvable group, and hence exhibits a Sylow system of the group. The algorithm is similar in pattern to those in Section 2. We present the algorithm as pseudocode in Figure 1 and include a proof of its correctness below.

We use the same notation as in the Sylow Complement System algorithm for the proof of the correctness. First note that if $z \in K_j$, then since $K_j \le C_{i+1}$ we have $a_i z$ in $C_i \setminus C_{i+1}$. Thus replacing a_i by $a_i z$ gives a polycyclic generating sequence that determines the same composition series $G = C_1 \rhd \ldots \rhd C_{n+1} = 1$.

For $i = n$, $\mathcal{A}$ exhibits a complement system of $C_{n+1} = 1$. We assert that if $\mathcal{A}$ exhibits a complement system of C_{i+1} before entering the inner **for** loop then $\mathcal{A}$ exhibits a complement system of C_i on exit from that loop. It will follow that $\mathcal{A}$ exhibits a complement system of $C_1 = G$ on exit from the outer loop.

Suppose that $\mathcal{A}$ exhibits a complement system of C_{i+1}. For convenience we introduce the terminology "H is an r-complement in $L \bmod K$" to mean that $K \le H \le L$ and that H/K is an r-complement of L/K. A complement system of $L \bmod K$ is a complete set of such subgroups of L. Since C_i/K_t is a p-group, $\mathcal{A}$ exhibits a complement system of $C_i \bmod K_t$. We will show that if $\mathcal{A}$ exhibits a complement system of $C_i \bmod K_j$ at the start of the inner loop, then $\mathcal{A}$ exhibits a complement system of $C_i \bmod K_{j+1}$ at the end

input: A polycyclic generating sequence $\mathcal{A} = (a_1, \ldots, a_n)$ determining the composition series $G = C_1 \rhd \ldots \rhd C_{n+1} = 1$ and refining the elementary abelian normal series $G = K_1 \rhd \ldots \rhd K_{m+1} = 1$.

output: A polycyclic generating sequence exhibiting a Sylow complement system.

```
for i = n down to 1 do
    Find t with K_{t-1} ≥ C_i > C_{i+1} ≥ K_t.
    for j = t to m do
        Let p = |C_i/C_{i+1}| and let q be the prime dividing [K_j : K_{j+1}].
        if p ≠ q then
            Let B be a set of generators for the q-complement R of C_{i+1} that A exhibits.
            Let a = a_i, and factor a^p = x · y and [b, a] = x_b · y_b for each b in B, with
                x and x_b in R and y and y_b in K_j.
            Let z in K_j be a solution mod K_{j+1} of the system of congruences
                z^{-1} · z^{-a} ··· z^{-a^{p-1}} ≡ y and z^{-1} · z^{b[b,a]} ≡ y_b for all b in B.
            Replace a_i by az.
        fi
    od
od
return A
```

Figure 1. Sylow Complement System

of the loop. It will follow that on exit from the loop $\mathcal{A}$ exhibits a complement system for $C_i \bmod K_{m+1}$, i.e., a complement system of C_i.

Thus suppose that $\mathcal{A}$ exhibits a complement system of C_{i+1} and also exhibits a complement system of $C_i \bmod K_j$ for some j with $t \geq j \geq m$. Let $p = [C_i : C_{i+1}]$ and let q be the prime dividing $[K_j : K_{j+1}]$.

We will modify $\mathcal{A}$ by replacing a_i by $a_i z$ for some z in K_j. Since $z \in K_j \leq C_{i+1}$, such a replacement does not change the subgroups of C_{i+1} that are exhibited. Hence the new polycyclic generating sequence will exhibit the same complement system of C_{i+1} that $\mathcal{A}$ does.

If $R_{p'}$ is the p-complement of C_{i+1} that $\mathcal{A}$ exhibits, then $R_{p'}K_{j+1}$ is a p-complement of $C_i \bmod K_{j+1}$ that $\mathcal{A}$ exhibits. Moreover, for primes $r \neq q$ the r-complement $S_{r'}$ of $C_i \bmod K_j$ that $\mathcal{A}$ exhibits is an r-complement of $C_i \bmod K_{j+1}$. Thus if $p = q$, then $\mathcal{A}$ already exhibits a complement system of $C_i \bmod K_{j+1}$ and no modification of $\mathcal{A}$ is required.

Suppose now that $p \neq q$. Since $R_{p'} \leq C_{i+1}$, the new $\mathcal{A}$ will still exhibit $R_{p'}K_{j+1}$. IF r is a prime such that $p \neq r \neq q$, then $\mathcal{A}$ exhibits an r-complement $S_{r'}$ of $C_i \bmod K_j$, which is also an r-complement of $C_i \bmod K_{j+1}$ since $r \neq q$. Since $\mathcal{A}$ exhibits a complement system of $C_i \bmod K_j$, it exhibits a p-Sylow subgroup of $C_i \bmod K_j$, which must contain a_i and, because $r \neq p$, must be contained in $S_{r'}$. Hence $a_i K_j \subseteq S_{r'}$. Since $\mathcal{A}$ exhibits $S_{r'} \cap C_{i+1}$, and since both a_i and $a_i z$ are in $S_{r'} \setminus C_{i+1}$, the new $\mathcal{A}$ will still exhibit the r-complement $S_{r'}$ of $C_i \bmod K_{j+1}$.

As we shall see below, the solutions of the system of congruences in the algorithm are precisely the elements z for which the polycyclic generating sequence obtained by replacing a_i by $a_i z$ exhibits a q-complement of $C_i \bmod K_{j+1}$. The issue here is whether K_j contains any such solutions. We now show that it does.

Let S be the q-complement of $C_i \bmod K_j$ and R the q-complement of C_{i+1} that $\mathcal{A}$ exhibits. Let T be a q-complement of C_i that contains R. Then $T \cap C_{i+1} = R$ and TK_j

is a q-complement of C_i mod K_j, so $S = (TK_j)^c = T^cK_j$ for some c in C_i. Moreover, $R^cK_j = (T \cap C_{i+1})^c K_j = (T^c \cap C_{i+1})K_j = (T^cK_j) \cap C_{i+1} = S \cap C_{i+1}$, a q-complement of C_{i+1} mod K_j exhibited by $\mathcal{A}$. Thus R^cK_j must be RK_j. Since both RK_{j+1} and R^cK_{j+1} are q-complements of C_{i+1} mod K_{j+1}, Corollary I(4.14)(c) of (Doerk and Hawkes, 1992) implies that $RK_{j+1} = R^{cu}K_{j+1}$ for some u in K_j.

We have $T^{cu}K_j = T^cK_j = S$. Also $a_i \in S$, since $p \neq q$ and $\mathcal{A}$ exhibits S. Hence there is a z in K_j with $a_iz \in T^{cu} \leq S$. Now R^{cu} is maximal normal in T^{cu} and $R^{cu} \leq {C_{i+1}}^{cu} = C_{i+1}$, so $a_iz \notin R^{cu}K_{j+1} = RK_{j+1}$. It follows that $\langle a_iz, RK_{j+1}\rangle = T^{cu}K_{j+1}$, that $(a_iz)^p \in RK_{j+1}$ and that a_iz normalizes RK_{j+1}, i.e., that the polycyclic generating sequence obtained from $\mathcal{A}$ by replacing a_i by a_iz exhibits the q-complement $T^{cu}K_{j+1}$ of C_i mod K_{j+1}.

For notational convenience, let $a = a_i$. Factor a^p into $x \cdot y$ with $x \in R$ and $y \in K_j$, and factor $[b, a]$ similarly into $x_b \cdot y_b$ for each $b \in B$, where $\langle B\rangle = R$. Since $(az)^p = a^p z^{a^{p-1}} \cdots z^a z$, we have

$$\begin{aligned} (az)^p \in RK_{j+1} \quad &\Longleftrightarrow \quad y z^{a^{p-1}} \cdots z^a z \in K_j \cap RK_{j+1} = K_{j+1} \\ &\Longleftrightarrow \quad y \equiv z^{-1} z^{-a} \cdots z^{-a^{p-1}} \bmod K_{j+1}. \end{aligned}$$

As we noted in Section 2.1, for each g in G the set of elements v of RK_{j+1} for which $[v, g] \in RK_{j+1}$ is a group. Hence az normalizes RK_{j+1} if and only if $[b, az] \in RK_{j+1}$ for every b in B. Since $[b, az] = x_b \cdot y_b \cdot [z, b^a]^{-1}$,

$$\begin{aligned} [b, az] \in RK_{j+1} \quad &\Longleftrightarrow \quad x_b \cdot y_b \cdot [z, b^a]^{-1} \in RK_{j+1} \\ &\Longleftrightarrow \quad y_b \equiv [z, b^a] \bmod K_{j+1}. \end{aligned}$$

These arguments show not only that K_j contains an element z satisfying the system of congruences but also that every solution of the system of congruences can be used to replace a_i by a_iz and exhibit a complement system of C_i mod K_{j+1}.

This completes the proof that the algorithm returns a complement system of G.

Acknowledgements. The first author's work on this paper was supported by the Graduiertenkolleg "Analyse und Konstruktion in der Mathematik" at RWTH Aachen. The second author especially wishes to thank the Deutsche Akademische Austauschdienst and the RWTH Aachen for their support during the preparation of this article. We are in debt to Joachim Neubüser for his help and his support on this project and to Klaus Lux for supplying us with a test group.

References

Cannon, J., Leedham-Green, C. R. (1993). Special presentations of finite soluble groups. Unpublished.

Carter, R. W., Hawkes, T. O. (1967). The $\mathfrak{F}$-normalizers of a finite soluble group. *J. Alg*, 5:175 – 201.

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

Doerk, K., Hawkes, T. O. (1992). *Finite soluble groups*. Walter de Gruyter.

Eick, B. (1997). Special presentations of finite soluble groups and computing (pre-) frattini subgroups. In Finkelstein, L., Kantor, W., editors, *DIMACS series 'Groups and Computation' 1996*. Amer. Math. Soc.

Gaschütz, W. (1963). Zur Theorie der endlichen auflösbaren Gruppen. *Math. Z.*, 80:300 – 305.

Laue, R., Neubüser, J., Schoenwaelder, U. (1984). Algorithms for finite soluble groups and the sogos system. In Atkinson, M. D., editor, *Proceedings of the LMS symposium on computational group theory, Durham 1982*, pages 105 – 135. Academic Press.

Niemeyer, A. C. (1994). A finite soluble quotient algorithm. *J. Symb. Comput.*, 18:541 – 561.

Plesken, W. (1987). Towards a soluble quotient algorithm. *J. Symb. Comput.*, 4:111 – 122.
Schönert, M. *et al.* (1995). *GAP - Groups, Algorithms and Programming*, Lehrstuhl D für Mathematik, Rheinisch Westfälische Technische Hochschule, Aachen, Germany, fifth edition.
Sims, C. C. (1990). Computing the order of a solvable permutation group. *J. Symb. Comput.*, 9:699 – 705.
Sims, C. C. (1994). *Computation with finitely presented groups.* Cambridge University Press.
Wright, C. R. B. (1973a). An internal approach to covering groups. *J. Alg.*, 25:128 – 145.
Wright, C. R. B. (1973b). On internal formation theory. *Math. Z.*, 134:1 – 9.