Available online at www.sciencedirect.com
SCIENCE DIRECT®

Journal of Symbolic Computation 38 (2004) 1445–1460

Journal of Symbolic Computation

www.elsevier.com/locate/jsc

# Special polycyclic generating sequences for finite soluble groups

John J. Cannon[a], Bettina Eick[b,*], Charles R. Leedham-Green[c]

[a] *School of Mathematics and Statistics, University of Sydney, Sydney, NSW 2006, Australia*
[b] *Institut Computational Mathematics, University of Braunschweig, 38106 Braunschweig, Germany*
[c] *School of Mathematical Sciences, Queen Mary and Westfield College, London, EI 4NS, UK*

Received 13 October 2003; accepted 25 May 2004

Available online 31 July 2004

**Abstract**

Polycyclic generating sequences are known to be a powerful tool in the design of practical and efficient algorithms for computing in finite soluble groups. Here we describe a further development: the so-called *special polycyclic generating sequences*. We give an overview of their properties and introduce a practical algorithm for determining a special polycyclic generating sequence in a given finite soluble group.


*Keywords:* Soluble groups; Maximal subgroups; Hall subgroups; Algorithmic group theory

## 1. Introduction

A finite group is soluble if and only if its composition factors are of prime order. Thus each finite soluble group is polycyclic and hence has a polycyclic generating sequence; that is, a generating set which exhibits a polycyclic series. Polycyclic generating sequences reflect the structure of the groups that they generate and they are a powerful tool in the design of practical and efficient algorithms for computing in finite soluble groups.

* Corresponding address: Institut Computational Mathematics, Universitat Braunschweig, Pockelsstrasse 14, 38106 Braunschweig, Germany. Tel.: +49 531 391 7525; fax: +49 531 391 8206.
*E-mail address:* beick@tu-bs.de (B. Eick).

0747-7171/$ - see front matter 
doi:10.1016/j.jsc.2004.05.003

There are also other characterisations known for finite soluble groups. For example, a finite group is soluble if and only if it has a system of Hall subgroups. And a finite group is soluble if and only if its chief factors are abelian. Further, each maximal subgroup of a finite soluble group complements a chief factor. The central position of Hall and maximal subgroups in the theory of finite soluble groups has long been recognised.

A *special polycyclic generating sequence* reflects the internal structure of the group that it defines more precisely than an arbitrary polycyclic generating sequence. For example, a special polycyclic generating sequence exhibits a system of Hall subgroups and it provides easy access to the maximal subgroups of the underlying group. This property can be used to improve the algorithmic theory for finite soluble groups.

The main aim here is to summarise an algorithm for determining a special polycyclic generating sequence for a given finite soluble group. A first version of the algorithm was devised in 1987 and developed over the next few years in Sydney, based on the computer algebra system Cayley (later Magma); see Cannon and Leedham-Green (1990). A first implementation in GAP was obtained in 1991; see Eick (1993). Both implementations were improved in 1994 by incorporating a method from Eick and Wright (2002). Here we provide a complete and unified report on the method.

Implementations of this algorithm are available in the computer algebra systems GAP (The Gap Group, 2000) and MAGMA (Bosma et al., 1997). Both implementations have shown that the algorithm described here is effective and can be used for various computations in finite soluble groups.

## 2. Special polycyclic generating sequences and applications

Let $G$ be a finite soluble group with composition series $G = C_1 \rhd \cdots \rhd C_n \rhd C_{n+1} = 1$. If we choose $a_i \in C_i \setminus C_{i+1}$ for $1 \leq i \leq n$, then we obtain a *polycyclic generating sequence* or *pcgs* $\mathcal{A} = (a_1, \ldots, a_n)$ of $G$. It follows that $C_i = \langle a_i, \ldots, a_n \rangle$ and thus the pcgs $\mathcal{A}$ determines its underlying composition series uniquely. Further, if $[C_i : C_{i+1}] = p_i$, then the prime $p_i$ is the *relative order* of the element $a_i$.

In general, a finite soluble group has many composition series and each composition series admits several choices for elements $a_1, \ldots, a_n$. For a special polycyclic generating sequence we shall require a 'good' choice for both as we will describe below. First, we need the following notation.

Let $\mathcal{A}$ be a pcgs of $G$. We say that $\mathcal{A}$ *refines* a series $G = N_1 \geq \cdots \geq N_l \geq N_{l+1} = 1$ if the composition series determined by $\mathcal{A}$ refines this series. In this case for each $j \in \{1, \ldots, l\}$ there exists an index $i_j$ such that the tail sequence $(a_{i_j}, \ldots, a_n)$ forms a pcgs of $N_j$. Note that for each subnormal series of $G$ there exists a pcgs $\mathcal{A}$ refining this series.

Let $U$ be a subgroup of $G$. We say that $U$ is *exhibited* by $\mathcal{A}$ if there exists a subsequence $(a_{i_1}, \ldots, a_{i_r})$ of $\mathcal{A}$ with $i_1 < \cdots < i_r$ which forms a pcgs of $U$. We denote such a subsequence by $U \cap \mathcal{A}$. If $\mathcal{A}$ refines a series of $G$, then each subgroup in this series is exhibited by $\mathcal{A}$. However, if $\mathcal{A}$ exhibits a subgroup $U$, then the series $G \geq U \geq 1$ is not necessarily refined by $\mathcal{A}$, as the pcgs $U \cap \mathcal{A}$ might not be a tail sequence of $\mathcal{A}$.

A special pcgs of $G$ is a pcgs with two additional properties: first, it refines the so-called *elementary abelian nilpotent-central series* of $G$ which is a characteristic series with elementary abelian factors introduced in Section 2.1 and, secondly, it exhibits a certain set of complement subgroups as described in Section 2.2.

### 2.1. *The elementary abelian nilpotent-central series*

Let $P$ be a finite $p$-group. The *lower exponent-$p$ central series* of $P$

$$P = \lambda_1(P) \rhd \lambda_2(P) \rhd \cdots \rhd \lambda_c(P) \rhd \lambda_{c+1}(P) = 1$$

is defined recursively by $\lambda_{i+1}(P) = [P, \lambda_i(P)]\lambda_i(P)^p$. This is a characteristic central series of $P$ with elementary abelian factors. The smallest integer $c$ with $\lambda_c(P) \neq 1$ and $\lambda_{c+1}(P) = 1$ is called the $p$-class of $P$.

Let $N$ be a finite nilpotent group. Then $N$ is a direct product of its Sylow subgroups, say $N = P_1 \times \cdots \times P_r$ for $P_i$ a $p_i$-group of $p_i$-class $c_i$. Let $c = \max\{c_1, \ldots, c_r\}$. By defining $\lambda_j(N) = \lambda_j(P_1) \times \cdots \times \lambda_j(P_r)$ we obtain a characteristic central series of $N$ whose factors are elementary; that is, the factors are direct products of elementary abelian groups. We call this series the *lower elementary central series*

$$N = \lambda_1(N) \rhd \lambda_2(N) \rhd \cdots \rhd \lambda_c(N) \rhd \lambda_{c+1}(N) = 1.$$

Let $G$ be a finite soluble group. We introduce the *lower nilpotent series* of $G$

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

where $G_{i+1}$ is the smallest normal subgroup of $G_i$ with a nilpotent factor group $G_i/G_{i+1}$. This is a characteristic series of $G$. The lower nilpotent series plays a similar role for a finite soluble group to that played by the lower central series for a nilpotent group.

The nilpotent-central series of $G$ is obtained by combining the above series. First, we consider the lower nilpotent series of $G$ and refine each factor in this series by its lower elementary central series. For this purpose we define subgroups $G_{i,j}$ by $G_{i,j}/G_{i+1} = \lambda_j(G_i/G_{i+1})$. Let $c_i$ be the length of the lower elementary central series of $G_i/G_{i+1}$. We obtain the series

$$\begin{aligned} G = G_1 = G_{1,1} \rhd G_{1,2} \rhd \cdots \rhd G_{1,c_1} \rhd G_{1,c_1+1} = {} \\ G_2 = G_{2,1} \rhd G_{2,2} \rhd \cdots \rhd G_{2,c_2} \rhd G_{2,c_2+1} = {} \\ \cdots = {} \\ G_m = G_{m,1} \rhd G_{m,2} \rhd \cdots \rhd G_{m,c_m} \rhd G_{m,c_m+1} = {} \\ G_{m+1} = G_{m+1,1} = 1. \end{aligned}$$

The resulting series is called the *nilpotent-central series*. It is a characteristic series of $G$ whose factors are direct products of elementary abelian groups. Using the Sylow subgroups of the factors we can refine each factor in the nilpotent-central series by a characteristic series with maximal elementary abelian factors. If we sort the Sylow $p$-subgroups of the factors in order of increasing primes $p$, then the resulting refined series is unique and we denote it as *elementary abelian nilpotent-central series* of $G$. (This series has been called the LG-series in Eick (1993) and Eick and Wright (2002).)

The factors $G_i/G_{i,2}$ of the nilpotent-central series series are called *heads* and the other factors of this series are called *tails*. Similarly, we call each factor of the elementary abelian nilpotent-central series which refines a head a *head factor* and each factor which refines a tail a *tail factor*.

### 2.2. Complement subgroups and special pcgs

A $p$-complement of the finite group $G$ is a subgroup $S^{(p)}$ such that $[G : S^{(p)}]$ is a $p$-power and $|S^{(p)}|$ is prime to $p$. Recall that by Hall's theorem in a finite soluble group $G$ a $p$-complement exists for each prime $p$ and all $p$-complements in $G$ for a fixed prime $p$ are conjugate in $G$.

Let $H_i = G_i/G_{i,2}$ be a head of the finite soluble group $G$. A *head complement* to $H_i$ in $G$ is a subgroup $K$ of $G$ with $KG_i = G$ and $K \cap G_i = G_{i,2}$. Note that $K_1 = G_{1,2}$ is a head complement for the first head. The head complements for the other heads have properties similar to the $p$-complements as observed in the following theorem.

**Theorem 1.** *Let $G$ be a finite soluble group and $H_i = G_i/G_{i,2}$ a head with $i > 1$.*

(a) $[H_i, G_{i-1}] = H_i$ *and* $C_{H_i}(G_{i-1}) = 1$.
(b) *There exists a head complement $K_i$ to $H_i$ in $G$ and all head complements to $H_i$ in $G$ are conjugate in $G$.*

**Proof.** Part (a) follows from the fact that $G_i$ is the smallest normal subgroup in $G_{i-1}$ with $G_{i-1}/G_i$ nilpotent. Part (b) follows from (a) by Theorem A in Robinson (1976), since $G_{i-1}/G_i$ is a nilpotent normal subgroup of $G/G_i$ acting in a fixed-point-free fashion on the abelian group $H_i$. □

**Definition 2.** The pcgs $\mathcal{A}$ of the finite soluble group $G$ is called *special* if it refines the elementary abelian nilpotent-central series of $G$ and exhibits simultaneously a $p$-complement for each prime $p$ and a head complement $K_i$ for each head $G_i/G_{i,2}$ for $1 \leq i \leq m$.

In Leedham-Green (1984) or in Eick (1997, Lemma 1.3), it is proved that special polycyclic generating sequences exist for each finite soluble group $G$. Our algorithm for computing special polycyclic generating sequences in Section 3 can be considered as another proof.

### 2.3. Properties and applications of special pcgs

Let $\pi_G$ be the set of prime divisors of $|G|$. A Hall system of $G$ is a set of Hall subgroups $\{S_\pi \mid \pi \subseteq \pi_G\}$ such that $S_{\pi_1} S_{\pi_2} = S_{\pi_1 \cup \pi_2}$ for each pair of sets $\pi_1, \pi_2 \subseteq \pi_G$. If for each $p \in \pi_G$ an arbitrary $p$-complement $S^{(p)}$ is given, then we can generate a Hall system of $G$ by defining $S_\pi = \cap_{p \in \pi_G \setminus \pi} S^{(p)}$. The following Lemma observes that a special pcgs exhibits each subgroup in the Hall system generated by the exhibited $p$-complements; see Eick and Wright (2002) for a proof.

**Lemma 3.** *Let $\mathcal{A}$ be a pcgs of a finite soluble group $G$ which exhibits subgroups $U$ and $V$ of $G$. Then $\mathcal{A}$ exhibits $U \cap V$ and, if $UV$ is a subgroup of $G$, then $\mathcal{A}$ exhibits $UV$.*

Another important property of special polycyclic generating sequences is their relation to maximal subgroups as outlined in the following lemma; see Eick (1997, Section 1.6), for a proof.

**Lemma 4.** *Let $G$ be a finite soluble group.*

(a) *For each maximal subgroup $M$ of $G$ there exists a unique head $G_i/G_{i,2}$ of $G$ which is not covered by $M$; that is, $G_i \not\leq MG_{i,2}$ or, equivalently, $G_{i,2} \leq M$ and $G_i \not\leq M$.*
(b) *Let $L_1, \ldots, L_r$ be the maximal $G$-normal subgroups of $G_i$ with $G_{i,2} \leq L_i$. Further, let $K_i$ be a head complement to $G_i/G_{i,2}$. Then $L_1K_i, \ldots, L_rK_i$ is a set of conjugacy class representatives for those maximal subgroups of $G$ not covering $G_i/G_{i,2}$.*

If a special pcgs $\mathcal{A}$ of a group $G$ is given, then a head complement $K_i$ for each head is exhibited by $\mathcal{A}$. Thus for determining the maximal subgroups of $G$ up to conjugacy it remains to compute the $G$-maximal subgroups for each head $G_i/G_{i,2}$. Since each such head is a direct product of elementary abelian $p$-groups, this can be translated into the computation of the maximal submodules of an $\mathbb{F}_pG$-module which, in turn, can be achieved effectively using the methods in Lux et al. (1994) or Holt et al. (1996). Hence a special pcgs is closely related to the maximal subgroups of the underlying group and the maximal subgroups can be determined easily once a special pcgs is given.

### *2.4. Example: A special pcgs for the symmetric group $S_4$*

Let $a_1 = (1, 2)$, $a_2 = (1, 2, 3)$, $a_3 = (1, 4)(2, 3)$ and $a_4 = (1, 3)(2, 4)$. We show that the sequence $\mathcal{A} = (a_1, \ldots, a_4)$ forms a special pcgs for the symmetric group $G = S_4$.

First, we consider the lower nilpotent series of $G$. By definition, $G = G_1$. Then $G_2 = \langle a_2, a_3, a_4\rangle \cong A_4$ and $G_3 = \langle a_3, a_4\rangle \cong V_4$, so $G_4 = 1$. Thus the lower nilpotent series is a chief series and cannot be refined. Hence the lower nilpotent series is the elementary abelian nilpotent-central series in this case.

Next, we observe that the $p$-complements are exhibited. Every 3-complement of $G$ is a dihedral group of order 8 and the subsequence $(a_1, a_3, a_4)$ forms a pcgs for such a group. Every 2-complement of $G$ is cyclic of order 3 and $(a_2)$ forms a pcgs for such a group.

Finally, we show that the head complements are exhibited. The head complement $K_1 = G_2$ is always exhibited by a pcgs refining the nilpotent-central series. Further, $H_2 = G_2/G_3 \cong C_3$. Thus each 3-complement is a head complement to $H_2$ and therefore a head complement to $H_2$ is exhibited. Also, $H_3 = G_3/G_4 \cong V_4$. We observe that the subsequence $(a_1, a_2)$ forms a pcgs for a head complement to $H_3$.

## 3. The determination of a special pcgs

Let $G$ be a finite soluble group. We determine a special pcgs for $G$ in two steps starting from an arbitrary pcgs $\mathcal{A}$. First, we modify $\mathcal{A}$ to a pcgs of $G$ which refines the elementary abelian nilpotent-central series of $G$; see Section 3.1. Then we adjust the resulting pcgs further so that a set of $p$-complements and a set of head complements are exhibited; see Section 3.2.

### *3.1. Refining the elementary abelian nilpotent-central series*

In this section we describe a process for modifying a given pcgs of a finite soluble group so that it refines the elementary abelian nilpotent-central series of $G$. First, the following lemma shows that it is sufficient to exhibit the subgroups in the elementary abelian nilpotent-central series of $G$ with a pcgs; a pcgs refining the series can then be obtained by reordering the elements.

**Lemma 5.** *Let $\mathcal{A}$ be a pcgs of $G$ which exhibits all subgroups of the normal series $G = N_1 \rhd \cdots \rhd N_l \rhd N_{l+1} = 1$. Let $\mathcal{B}$ be the concatenation of the following sequences:*

$$\mathcal{A} \cap N_1 \setminus N_2, \ldots, \mathcal{A} \cap N_i \setminus N_{i+1}, \ldots, \mathcal{A} \cap N_l.$$

*Then $\mathcal{B}$ is a pcgs of $G$ which refines the given normal series.*

**Proof.** $\mathcal{A} \cap N_l$ is a pcgs of $N_l$, since $N_l$ is exhibited by $\mathcal{A}$. Moreover, since $N_l$ is a normal subgroup of $G$, the sequence $\mathcal{A} \setminus N_l$ induces a pcgs of $G/N_l$ which, by induction, exhibits the subgroups $N_i/N_l$ for all $i$. □

Let $g$ be an element of $G$ with $|g| = p_1^{e_1} \cdots p_r^{e_r}$. The *prime-power components* of $g$ are a list of commuting elements $g_1, \ldots, g_r$ with $g = g_1 \cdots g_r$ and $|g_i| = p_i^{e_i}$. Each $g_i$ is a uniquely determined power of $g$. If $g$ is trivial, then its prime-power components are defined as the empty list.

If a pcgs consists of prime-power elements only, then we call it a *prime-power pcgs*. If $\mathcal{A}$ is a given arbitrary pcgs, then we can easily derive a prime-power pcgs from $\mathcal{A}$: we substitute for each $a_i \in A$ its $p_i$-power component, where $p_i$ is the relative order of $a_i$.

It is straightforward to show that in an abelian group a prime-power pcgs exhibits the Sylow subgroups. This yields the following.

**Remark 6.** A prime-power pcgs of $G$ exhibits the nilpotent-central series of $G$ if and only if it exhibits the elementary abelian nilpotent-central series of $G$.

#### *3.1.1. Exhibiting a normal series using weights*

Let $G = N_1 \rhd \cdots \rhd N_l \rhd N_{l+1} = 1$ be an arbitrary normal series and suppose that a pcgs for each subgroup $N_i$ is given. In this section we describe a method for modifying a given arbitrary pcgs $\mathcal{A}$ of $G$ such that it exhibits this series.

We introduce weights for the elements of $G$ relative to the given normal series. If $g \in N_i$, then $w(g) = i$ is *an admissible weight* for $g$. If $g \in N_i$ and $g \notin N_{i+1}$, then $w_f(g) = i$ is *the final weight* of $g$. Thus the final weight of $g$ is uniquely defined, while each weight $u$ with $1 \le u \le w_f(g)$ is admissible for $g$. Additionally, we define $w_f(1) = l + 1$.

Let $\mathcal{A} = (a_1, \ldots, a_n)$ be a pcgs of $G$ and let $\mathcal{W} = (w_1, \ldots, w_n)$ be a sequence of admissible weights for the elements in $\mathcal{A}$. Let $G = C_1 \rhd \cdots \rhd C_n \rhd C_{n+1} = 1$ be the composition series determined by $\mathcal{A}$. Consider an element $g \in G$ with admissible weight $u$. A modification of $\mathcal{A}$ by $g$ is a routine which changes $\mathcal{A}$ and $\mathcal{W}$ in place as defined in Fig. 1.

Note that if $g = 1$, then the list of prime-power components of $g$ is empty and hence $\mathcal{A}$ remains unchanged in this case. Further properties of the algorithm ModifyPcgs are listed in the following lemma.

```
ModifyPcgs( A, W, g, u )
    for each prime-power component k of g do
        find d so that k = a_d^{e_d} · h with 0 < e_d < p_d and h ∈ C_{d+1}
        if w_d < u then
            replace a_d by k in A and w_d by u in W
        end if
        ModifyPcgs( A, W, h, min{u, w_d} )
    end for
```

Fig. 1. The modification of a pcgs.

**Lemma 7.** *Let $\mathcal{A} = (a_1, \ldots, a_n)$ be a pcgs with admissible weights $\mathcal{W} = (w_1, \ldots, w_n)$. Let $\mathcal{A}'$ and $\mathcal{W}'$ be the modified sequences after a call of ModifyPcgs( $\mathcal{A}, \mathcal{W}, g, u$ ).*

(a) *$\mathcal{A}'$ is a pcgs of $G$. If $\mathcal{A}$ is a prime-power pcgs, then $\mathcal{A}'$ is a prime-power pcgs.*
(b) *$\mathcal{W}'$ is a sequence of admissible weights for $\mathcal{A}'$ with $w_i \leq w_i'$ for $1 \leq i \leq n$.*
(c) *The element $g$ and each $a_i$ can be written as words in elements of $\mathcal{A}'$ which have admissible weight at least $u$ or $w_i$, respectively.*

**Proof.** (a) Consider an element $k \in G$ with $k = a_d^{e_d} \cdot h$. If we replace $a_d$ by $k$, then the resulting sequence is still a pcgs of $G$, since $k \in C_d \setminus C_{d+1}$. If $\mathcal{A}$ is a prime-power pcgs and $k$ has prime-power order, then the changed pcgs is a prime-power pcgs.
(b) Let $u$ be an admissible weight for $g$ and let $k$ be a prime-power component of $g$. Then $k = g^l$ for some $l$. Hence $u$ is an admissible weight for $k$ as well. Moreover, if $k = a_d^{e_d} \cdot h$, then $h = a_d^{-e_d} \cdot k$ and thus $\min\{u, w_d\}$ is an admissible weight for $h$. Hence in all steps of the algorithm we replace elements by elements with admissible weights only. Note that the weights can only increase in a modification step.
(c) First we consider $g$. Since $g$ is the product of its prime-power components and each prime-power component is a power of $g$, it follows that $g$ can be written as a product of elements of admissible weight at least $u$ if and only if this holds for each prime-power component of $g$. Hence we consider a prime-power component $k$ of $g$. The element $k$ is of the form $k = a_d^{e_d} \cdot h$ for some $h \in C_{d+1}$. If $a_d$ is replaced by $k$, then obviously $k$ can be written as a word in elements of $\mathcal{A}'$ as desired. If $a_d$ is not replaced, then $w_d \geq u$ and it remains to show that $h$ can be written as a word in elements of $\mathcal{A}'$ which have admissible weight at least $u$. However, since $h$ has a higher depth than the depth of $k$, we can assume by induction that this is true for $h$. Similarly, we can observe that $a_d = (k \cdot h^{-1})^l$ for $le_d \equiv 1 \bmod p_d$ can be written in elements with weight at least $w_d$. □

**Lemma 8.** *Let $\mathcal{A}$ be a prime-power pcgs of $G$ with admissible weights $\mathcal{W} = (1, \ldots, 1)$.*

(a) *Let $N$ be a normal subgroup of $G$ with pcgs $\mathcal{B} = (b_1, \ldots, b_l)$. We consider weights relative to the normal series $G \rhd N \rhd 1$. If we modify $\mathcal{A}$ successively by each of the elements $b_i$ with admissible weights $w(b_i) = 2$, then we obtain a prime-power pcgs $\mathcal{A}'$ of $G$ which exhibits $N$.*
(b) *Let $G = N_1 \rhd N_2 \rhd \cdots \rhd N_l \rhd N_{l+1} = 1$ be a normal series of $G$ and let $\mathcal{B}_j$ be a pcgs of $N_j$ for $1 \leq j \leq l$. We assign the admissible weight $j$ to each element of $\mathcal{B}_j$. If we modify $\mathcal{A}$ by each element of $\mathcal{B}_j$ for each $j \geq 2$, then we obtain a prime-power pcgs $\mathcal{A}'$ of $G$ which exhibits the normal series.*

**Proof.** (a) It follows from Lemma 7(a) that $\mathcal{A}'$ is a prime-power pcgs of $G$. Further, the modification procedure yields a list of weights $\mathcal{W}'$ for $\mathcal{A}'$. Since $\mathcal{W}'$ contains weights which are admissible by Lemma 7(b), the elements of $\mathcal{A}'$ having weight 2 are contained in $N$. By Lemma 7(c) they generate $N$. It remains to observe that they form a pcgs for $N$. We use induction on $l$ and suppose that a pcgs of $M = \langle b_2, \ldots, b_l \rangle$ is exhibited by $\mathcal{A}'$. By Lemma 7(a) the element $b_1$ is a word in elements of $\mathcal{A}'$ of weight 2. But $b_1 \notin M$. Thus there exists an element $a_d$ of weight 2 in $\mathcal{A}'$ with $a_d \in N \setminus M$. Hence $\mathcal{A}'$ exhibits $N$.
(b) This follows by an iterated application of (a). $\square$

### 3.1.2. Power–commutator series

Let $G$ be finite soluble group with prime-power pcgs $\mathcal{A} = (a_1, \ldots, a_n)$ and let $p_i$ denote the relative order of $a_i$ for $1 \le i \le n$. A normal subgroup $N$ of $G$ is called *power–commutator subgroup with respect to* $\mathcal{A}$ if $N$ is generated as normal subgroup in $G$ by the set $\{a_i^{p_i}, [a_i, a_j] \mid 1 \le i < j \le n\} \cap N$. Further, if $N$ is a power–commutator subgroup with respect to every prime-power pcgs $\mathcal{A}$ of $G$, then we call $N$ a *power–commutator subgroup* of $G$. The most straightforward example for a power–commutator subgroup of $G$ is the derived subgroup $G'$.

We extend the notation of power–commutator subgroups to subgroup series of $G$ using a recursive definition: we call a normal series $G = N_1 \rhd \cdots \rhd N_l \rhd N_{l+1} = 1$ a *power–commutator series* of $G$ if the subgroup $N_{c+1}$ is a power–commutator subgroup of $G$ with respect to every prime-power pcgs $\mathcal{A}$ of $G$ which exhibits $N_1, \ldots, N_c$. Thus, in particular, $N_2$ is a power–commutator subgroup of $G$.

Again, the most obvious example for a power–commutator series is the derived series of $G$: if the $c$-th subgroup $G^{(c)}$ in this series is exhibited by $\mathcal{A}$, then $G^{(c+1)}$ is generated by all commutators of elements in $\mathcal{A} \cap G^{(c)}$ and thus $G^{(c+1)}$ is a power–commutator subgroup with respect to $\mathcal{A}$. Other straightforward examples for power–commutator subgroups include the lower central series and the lower elementary central series of a finite nilpotent groups and the Jennings series of a finite $p$-group. Later we observe that the lower nilpotent series and the nilpotent-central series are also power–commutator series.

### 3.1.3. Weight functions for power–commutator series

A power–commutator series can be defined using a weight function; that is, a function that takes as input a prime-power pcgs $\mathcal{A}$ exhibiting $N_1, \ldots, N_c$ and determines a set of powers and commutators of $\mathcal{A}$ which generate $N_{c+1}$ as a normal subgroup. This information can then be used to modify $\mathcal{A}$ so that $N_{c+1}$ is exhibited by $\mathcal{A}$ as well. Hence we obtain a pcgs $\mathcal{A}$ that satisfies the hypothesis for the next inductive step in exhibiting the full series $N_1, \ldots, N_{l+1}$. A more precise outline for this iterated modification method will be given in Fig. 2 below.

Before, we consider the definition of weight functions for power–commutator series in more detail. The input to such a function is a prime-power pcgs $\mathcal{A}$ which exhibits $N_1, \ldots, N_c$. Thus for each $k \in \{1, \ldots, c\}$, there exists a subset of $\mathcal{A}$ which is a pcgs of $N_k$. For the determination of the powers and commutators in $N_{c+1}$, the weight function needs to know the integer $c$ and the subsets of $\mathcal{A}$ forming pcgs for $N_1, \ldots, N_c$. We exhibit these subsets using a list of weights $\mathcal{W}$. In fact, this list $\mathcal{W} = (w_1, \ldots, w_n)$ corresponds to $\mathcal{A} = (a_1, \ldots, a_n)$ and it serves two purposes:

- Each weight $w_i$ is admissible for $a_i$ with respect to the series $N_1, \ldots, N_{l+1}$; that is, $a_i \in N_{w_i}$ for $1 \le i \le n$.
- The subsequence $(a_i \mid w_i \ge k)$ is a pcgs of $N_k$ for $1 \le k \le c$; that is, the weights $w_i \le c$ are final weights.

Note that these two requirements are compatible with each other.

Using such a list of weights $\mathcal{W}$ we can now explicitly consider a function 'AdmissibleWeight( $\mathcal{A}, \mathcal{W}, c, i, j$ )' which returns a weight $w(i, j)$ for the element $g = a_i^{p_i}$ if $i = j$ or for $g = [a_i, a_j]$ if $i \neq j$. The weight $w(i, j)$ has to be admissible for $g$; that is, $g \in N_{w(i,j)}$. Further, we require:

(1) $w(i, j) \ge \max\{w_i, w_j\}$ for $i, j \in \{1, \ldots, n\}$.
(2) $N_{c+1}$ is generated as a normal subgroup in $G$ by the set $\{a_i^{p_i}, [a_i, a_j] \mid w(i, j) \ge c + 1\}$.

Condition (1) can always be satisfied, since the underlying series $N_1, \ldots, N_{l+1}$ is a normal series of $G$. This condition is used to ensure that the weight function is making progress in increasing the weights.

Condition (2) yields that sufficiently many powers and commutators obtain a weight at least $c + 1$ so that we obtain a normal subgroup generating set of $N_{c+1}$.

*3.1.4. Exhibiting a power–commutator series with a weight function*

Now we are in the position to outline an algorithm which can be used to modify a given prime-power pcgs of $G$ such that it exhibits a power–commutator series $G = N_1 \rhd \cdots \rhd N_l \rhd N_{l+1} = 1$ which is described by a function 'AdmissibleWeight'. Our approach proceeds by induction downwards the series considered. In the inductive step we assume that we have a prime-power pcgs $\mathcal{A}$ of $G$ exhibiting $N_1, \ldots, N_c$ and we want to modify $\mathcal{A}$ such that $N_{c+1}$ is exhibited additionally.

In Fig. 2 we present a top-level outline of the algorithm used to exhibit the next subgroup $N_{c+1}$ in the implicitly given power–commutator series of $G$. The outline of the algorithm incorporates a function 'IsUseful' which is used for efficiency reasons. At this stage the reader might assume that this function returns true on all inputs. We discuss the efficiency of the algorithm in more detail below.

Next, we can use 'ExhibitNextSubgroup' as outlined in Fig. 2 to exhibit a power–commutator series of $G$ as we show in Fig. 3. Note that it is not necessary to know the length of the given power–commutator series a priori. Note also that a power–commutator series is defined to end at the trivial subgroup. This ensures that each element in a pcgs has a maximal admissible weight, which is necessary for the following algorithm to terminate.

**Lemma 9.** *If $\mathcal{A}$ is a prime-power pcgs with admissible weights $\mathcal{W}$ such that $\mathcal{A}$ exhibits $N_1, \ldots, N_c$, then 'ExhibitNextSubgroup' modifies $\mathcal{A}$ and $\mathcal{W}$ in place such that $N_{c+1}$ is exhibited as well.*

**Proof.** Suppose by induction that the elements of weight at least $k$ form a pcgs of $N_k$ for $1 \le k \le c$ in $\mathcal{A}$. Let $\mathcal{A}'$ and $\mathcal{W}'$ be the modified sequences. Using Lemma 7 we observe that $\mathcal{A}'$ is a prime-power pcgs for $G$ with admissible weights $\mathcal{W}'$. Thus, since $\mathcal{W} \le \mathcal{W}'$, the subgroups $N_1, \ldots, N_c$ are still exhibited by $\mathcal{A}'$. By condition (2) on 'AdmissibleWeight', the elements in $\mathcal{A}'$ of weight at least $c + 1$ generate $N_{c+1}$ as normal subgroup.

```
ExhibitNextSubgroup( 𝒜, 𝒲, c, AdmissibleWeight )
    unmark all elements in 𝒜
    while there is an unmarked element in 𝒜 do
        find the smallest i with a_i unmarked and mark a_i
        for j from 1 to i do
            let u = AdmissibleWeight( 𝒜, 𝒲, c, i, j )
            if u > c and IsUseful( i, j, u ) then
                if i = j then
                    g = a_i^{p_i}
                else
                    g = [a_i, a_j]
                end if
                ModifyPcgs( 𝒜, 𝒲, g, u )
                unmark each a_k in 𝒜 changed by ModifyPcgs
            end if
        end for
    end while
```

Fig. 2. Exhibiting the next subgroup in a power–commutator series.

```
ExhibitSeries( 𝒜, AdmissibleWeight )
    let 𝒲 = (1, ..., 1) be the initial admissible weights for 𝒜
    initialise counters m = 1 and c = 1
    while c ≤ m + 1 do
        ExhibitNextSubgroup( 𝒜, 𝒲, c, AdmissibleWeight )
        reset c = c + 1
        reset m to the maximum in 𝒲
    end while
    return 𝒜 and 𝒲
```

Fig. 3. Exhibiting a power–commutator series.

We use Lemma 8 to show that these elements form in fact a pcgs for $N_{c+1}$; that is, we show that we modify $\mathcal{A}$ by a pcgs of $N_{c+1}$ so that $N_{c+1}$ is exhibited by $\mathcal{A}'$. If $a_i, a_j \in \mathcal{A}'$ are elements of weight $c+1$, then by condition (1) we observe that $a_i^{p_i}$ and $[a_i, a_j]$ obtain weight of at least $c+1$. Thus the set of elements in $\mathcal{A}'$ of weight at least $c+1$ is closed under taking powers and commutators. Hence, as observed in Laue et al. (1984), the elements in $\mathcal{A}'$ of weight at least $c+1$ form a pcgs of a subgroup. Further, again by condition (1), the set of elements of weight $c+1$ is closed under conjugation by each generator of $G$ and hence forms a pcgs of a normal subgroup of $G$. Thus the elements in $\mathcal{A}'$ form a pcgs for $N_{c+1}$. □

Hence the algorithm 'ExhibitSeries' can be used to exhibit an implicitly given power–commutator series of $G$. Now we consider the efficiency of this algorithm in more detail. First we introduce the look-ahead feature.

**Remark 10.** AdmissibleWeight( $\mathcal{A}, \mathcal{W}, i, j, c$ ) might also return weights greater than $c+1$ which may be considered as a *look-ahead*. This feature can be used to increase the efficiency of the algorithm, since the admissible weights converge faster towards their final weights using this feature.

Then we consider the use of the function 'IsUseful' in more detail. The first purpose of 'IsUseful' is to prevent the algorithm from trying to modify $\mathcal{A}$ by elements $g$ with weight $u$ which have been considered before. Thus 'IsUseful' carries a look-up table in the background where we note which powers, commutators and weights have been considered. If the algorithm considers the same power or commutator with some weight for a second time, then 'IsUseful' returns false.

'IsUseful' might be used for further reductions depending on the power–commutator series. We will include some examples for such reductions below.

*3.1.5. Admissible weights for the derived series*

We give an example of AdmissibleWeight for the derived series of $G$. Suppose that a pcgs for the $c$-th term $G^{(c)}$ of the derived series of $G$ is exhibited by $\mathcal{A}$. Then $G^{(c+1)}$ is generated as a normal subgroup by the elements $[a_i, a_j]$ for $1 \leq j < i \leq n$ with $w_i \geq c$.

AdmissibleWeight-DerivedSeriesI( $\mathcal{A}, \mathcal{W}, i, j, c$ )
  If $i \neq j$ and $w_i = w_j = c$, then return $c + 1$.
  Otherwise return $\max\{w_i, w_j\}$.

We give another weight function corresponding to the derived series which uses the look-ahead feature and thus increases the efficiency of the algorithm 'ExhibitingSeries'. Note that it is important for this second version to ensure that 'IsUseful' returns false if we consider a power or commutator with known weight again.

AdmissibleWeight-DerivedSeriesII( $\mathcal{A}, \mathcal{W}, i, j, c$ )
  If $i \neq j$ and $w_i = w_j \geq c$, then return $w_i + 1$.
  Otherwise return $\max\{w_i, w_j\}$.

By Glasby (1987) we observe that the elements $[a_i, a_j]$ for $1 \leq j < i \leq n$ with $w_i \geq c$ generate $G^{(c+1)}$. Hence we do not need to consider elements of weight less than $c$ at all. Thus we can reduce further the number of powers and commutators considered using the function 'IsUseful': we require that 'IsUseful( $i, j, u$ )' returns false if $w_i < c$ or $w_j < c$. Further, we do not need to consider commutators $[a_i, a_j]$ if $w_i \neq w_j$, since we do not need to close the generating set under conjugation. This can also be achieved using 'IsUseful'.

*3.1.6. Admissible weights for the lower nilpotent series*

First we show that the lower nilpotent series is a power–commutator series.

**Theorem 11.** *Let $G$ be a finite soluble group with prime-power pcgs $\mathcal{A} = (a_1, \ldots, a_n)$.*

(a) *$G$ is nilpotent if and only if $[a_i, a_j] = 1$ for each pair of elements $a_i$ and $a_j$ in $\mathcal{A}$ of coprime order.*
(b) *$G_2$ is generated by $\{[a_i, a_j] \mid 1 \leq i < j \leq n$ with $(|a_i|, |a_j|) = 1\}$ as a normal subgroup of $G$.*

**Proof.** Part (a) $\Rightarrow$: If $G$ is nilpotent, then $G$ is a direct product of its Sylow subgroups. Hence each two elements of coprime order commute and this part of the theorem is proved. Part (a) $\Leftarrow$: $G$ is nilpotent if and only if each Sylow subgroup of $G$ is normal. Let $p$ be a fixed prime and consider the $p$-elements in $\mathcal{A}$. We show that these elements generate a normal Sylow $p$-subgroup $S$ of $G$.

We use induction on $|\mathcal{A}|$ and consider $\mathcal{A}_2 = (a_2, \ldots, a_n)$. This is a pcgs of $C_2$, the second term of in the associated composition series of $G$, and it satisfies the assumption of the theorem. Thus the subgroup $T$ of $C_2$ generated by the $p$-elements in $\mathcal{A}_2$ is a normal Sylow $p$-subgroup of $C_2$ by induction. Hence $T$ is characteristic in $C_2$ and thus normal in $G$.

Recall that $[G : C_2] = q$ prime. If $q \neq p$, then $T$ is the subgroup $G$ generated by the $p$-elements in $\mathcal{A}$ and it is a normal Sylow $p$-subgroup of $G$. Thus we only have to consider the case $q = p$. In this case $a_1$ is a $p$-element. Let $S = \langle a_1, T\rangle$ be the subgroup of $G$ generated by the $p$-elements in $\mathcal{A}$. The element $a_1^p$ is a $p$-element of $C_2$ and thus $a_1^p \in T$. Thus $|S| = |T| \cdot p$ and hence $S$ is a Sylow $p$-subgroup of $G$. To show that $S$ is normal, consider $S^{a_j}$ for some $j$. If $a_j$ is a $p$-element of $G$, then $a_j \in S$ and thus $S^{a_j} = S$. If $a_j$ is a $p'$-element, then it commutes with each $p$-element in $\mathcal{A}$ by the assumption of the theorem and thus it centralises $S$. Hence $S^{a_j} = S$ in all cases and $S$ is normal in $G$.
Part (b) Let $L$ be the normal subgroup of $G$ generated by commutators of elements in $\mathcal{A}$ of coprime order. Note that $L \leq G_2$, since $G/G_2$ is nilpotent and elements of coprime order commute in $G/G_2$. Now consider the pcgs of $G/L$ induced by $\mathcal{A}$. This is a pcgs consisting of elements of prime-power order and each two coprime elements commute. Hence by (a) $G/L$ is nilpotent and thus $L = G_2$. $\square$

This result can be used to define a weight function which facilitates the exhibition of the lower nilpotent series using the algorithm ‘ExhibitingSeries’. Note that here we need the fact that we compute with a pcgs $\mathcal{A}$ which is a prime-power pcgs. As usual, we denote the prime dividing the order of $a_i$ by $p_i$.

AdmissibleWeight-LowerNilpotentSeries( $\mathcal{A}, \mathcal{W}, c, i, j$ )
If $i \neq j$ and $w_i = w_j \geq c$ and $p_i \neq p_j$, then return $w_i + 1$.
Otherwise return $\max\{w_j, w_j\}$.

*3.1.7. Admissible weights for the lower elementary central series*

Now we can approach the exhibition of the lower elementary central series of a finite nilpotent group. We can exhibit other kinds of central series of a finite nilpotent group in a similar form.

**Lemma 12.** *Let $P$ be a $p$-group.*

(a) *Let $\mathcal{A}$ be a pcgs of $P$. Then $\lambda_2(P) = \langle [a_i, a_j], a_i^p \mid 1 \leq i < j \leq n\rangle$.*
(b) *If $a \in \lambda_i(P)$ and $b \in \lambda_j(P)$, then $[a, b] \in \lambda_{i+j}(P)$.*

AdmissibleWeight-LowerElementaryCentralSeries( $\mathcal{A}, \mathcal{W}, c, i, j$ )
If $i = j$ and $w_i \geq c$ then return $w_i + 1$.
If $i \neq j$ and $w_i = w_j \geq c$ then return $w_i + w_j$.
Otherwise return $\max\{w_j, w_j\}$.

Again, we note that the powers and commutators of weight at least $c + 1$ form a generating set of $N_{c+1}$. Thus it is not necessary to close the elements of weight at least $c + 1$ under conjugation with the generators of $G$. The function ‘IsUseful’ can be used to facilitate this improvement.

*3.1.8. Admissible weights for the nilpotent-central series*

Now we want to combine the approaches of the Sections 3.1.6 and 3.1.7 to obtain a pcgs exhibiting the nilpotent-central series. Here we use a call of 'ExhibitNextSubgroup' to exhibit the next subgroup $G_{c+1}$ in the lower nilpotent series and, simultaneously, we refine $G_{c-1}/G_c$ by the lower elementary series and exhibit the refined series.

As admissible weights we use ordered pairs $(i, j)$ with lexicographic sorting corresponding to the subgroups in the nilpotent-central series $G_{i,j}$. We combine the weight functions of Sections 3.1.6 and 3.1.7 as follows.

AdmissibleWeight-NilpotentCentralSeries( $\mathcal{A}$, $\mathcal{W}$, $i$, $j$, $c$ )
  If $i \neq j$ and $w_i(1) = w_j(1) \geq c$ and $p_i \neq p_j$, then return $(w_i(1) + 1, 1)$.
  If $i = j$ and $w_i(1) = c - 1$, then return $(w_i(1), w_i(2) + 1)$.
  If $i \neq j$ and $w_i(1) = w_j(1) = c - 1$, then return $(c - 1, w_i(2) + w_j(2))$.
  Otherwise return $\max\{w_j, w_j\}$.

*3.2. Exhibiting complement subgroups*

Let $\mathcal{A} = (a_1, \ldots, a_n)$ be a prime-power pcgs of $G$ which refines the elementary abelian nilpotent-central series of $G$. In this section we show how to adjust $\mathcal{A}$ so that it exhibits a $p$-complement of $G$ for each prime $p$ and a head complement for each head of $G$ in addition to the elementary abelian nilpotent-central series.

Our algorithm proceeds by induction down the elementary abelian nilpotent-central series of $G$. Let $L$ be the smallest non-trivial subgroup in the elementary abelian nilpotent-central series of $G$. Since $\mathcal{A}$ refines the elementary abelian nilpotent-central series, $\mathcal{A} \cap L = (a_{r+1}, \ldots, a_n)$ is a pcgs of $L$. Thus $\overline{\mathcal{A}} = (a_1 L, \ldots, a_r L)$ is a pcgs of $G/L$ which refines the elementary abelian nilpotent-central series of $G/L$. By induction we assume that $\overline{A}$ exhibits a set of complement subgroups in $G/L$. In the following lemma we outline the relations between the complement subgroups of $G/L$ and $G$. The straightforward proof of the lemma is left to the reader.

**Lemma 13.** *Let $L$ be the smallest non-trivial subgroup in the elementary abelian nilpotent-central series of the finite soluble group $G$.*

(a) *By construction, $L$ is an elementary abelian $p$-group for a prime $p$. Let $S/L$ be a $q$-complement of $G/L$.*
  – *If $p \neq q$, then $S$ is a $q$-complement of $G$.*
  – *If $p = q$, then each complement to $L$ in $S$ is a $p$-complement of $G$.*

(b) *By construction $L \leq G_m$ and thus either $L \leq G_{m,2}$ or $G_{m,2} = 1$.*
  – *Let $j \in \{1, \ldots, m-1\}$. If $K/L$ is a $j$-head complement in $G/L$, then $K$ is a $j$-head complement in $G$.*
  – *Suppose that $L \leq G_{m,2}$. If $K/L$ is an $m$-head complement in $G/L$, then $K$ is an $m$-head complement in $G$.*
  – *Suppose that $G_{m,2} = 1$. If $K/L$ is an $m$-head complement in $G/L$, then each complement to $L$ in $K$ is an $m$-head complement in $G$.*

Note that a subgroup $U \leq G$ with $L \leq U$ is exhibited by $\mathcal{A}$ if and only if $U/L$ is exhibited by $\overline{A}$. Thus using Lemma 13 we observe that in each inductive step down the elementary abelian nilpotent-central series of $G$ we have to consider two cases:

**Case 1.** If $L \leq G_{m,2}$, then head complements for each head of $G$ are already exhibited by Lemma 13(a). Hence by Lemma 13(c) it remains to exhibit a $p$-complement of $G$. Such a $p$-complement can be obtained by exhibiting a complement to $L$ in $S$ where $S/L$ is the $p$-complement of $G/L$ exhibited by $\overline{\mathcal{A}}$.

**Case 2.** If $G_{m,2} = 1$, then $L$ is a head factor. In this case Lemma 13 yields that we have to exhibit additionally a head complement to $G_m$ and a $p$-complement. However, in the next lemma we show that it is sufficient to exhibit the head complement only and the $p$-complement follows automatically by Lemma 3.

**Lemma 14.** *Let $L$ be the smallest non-trivial subgroup in the elementary abelian nilpotent-central series of $G$. Suppose that $G_{m,2} = 1$ and recall that $G_m$ is a direct product of elementary abelian groups with Sylow $p$-subgroup $L$, say $G_m = L \times R$. If $S/L$ is a $p$-complement of $G/L$ and $K$ is a head complement to $G_m$, then $(S \cap K)R$ is a $p$-complement of $G$.*

**Proof.** First note that $G_m \leq S$ and thus $KS = G$. Hence $|S \cap K| = |S||K|/|SK| = |S|/|G_m|$ and $S \cap K$ is a $p$-complement of $K$. Note that $R$ is a $p$-complement of $G_m$ and $R$ is normal in $G$. Thus $|(S \cap K)R| = |S \cap K||R|$ and $(S \cap K)R$ is a $p$-complement of $G$. □

Hence in each of the above cases we have to exhibit just one additional subgroup and this additional subgroup can be described as a complement to $L$ in a subgroup which is already exhibited. Thus there exists a modification of $\mathcal{A}$ to a sequence of the form $\mathcal{A}' = (a_1 l_1, \ldots, a_r l_r, a_{r+1}, \ldots, a_n)$ with suitable elements $l_i \in L$ such that $\mathcal{A}'$ exhibits the desired additional subgroup of $G$. Note that any such sequence $\mathcal{A}'$ refines the elementary abelian nilpotent-central series of $G$ and exhibits all subgroups $U$ of $G$ where $U/L$ is exhibited by $\overline{\mathcal{A}}$. Thus the properties of $\mathcal{A}$ which have been achieved in earlier steps of the induction are preserved in $\mathcal{A}'$.

The following lemma yields the fundamental equations for determining suitable elements $l_i \in L$. Note that all the equations obtained in the following lemma translate into an inhomogeneous system of linear equations over a finite field, since $L$ is an elementary abelian group.

**Lemma 15.** *Let $G$ be a group and $L \trianglelefteq G$ an abelian normal subgroup.*

(a) *Let $g, h \in G$ with $[h, g] = s \cdot r$ for $r \in L$. Further, let $l \in L$.*
*Then $[h, gl] = s$ if and only if $l^a = r$ for $a = hs - 1$.*
(b) *Let $g \in G$ with $g^q = s \cdot r$ for $r \in L$. Further, let $l \in L$.*
*Then $(gl)^q = s$ if and only if $l^b = r$ for $b = -\sum_{i=0}^{q-1} g^i$.*

**Proof.** We use the following two equations:

$$[h, gl] = h^{-1} \cdot l^{-1} \cdot g^{-1} \cdot h \cdot g \cdot l = (l^{-1})^h \cdot [h, g] \cdot l = (l^{-1})^h \cdot s \cdot r \cdot l = s \cdot (l^{-1})^{hs} \cdot l \cdot r$$

$$(gl)^q = g \cdot l \cdot g \cdots g \cdot l = g^q \cdot l^{g^{q-1}} \cdot l^{g^{q-2}} \cdots l = s \cdot r \cdot l^{g^{q-1}} \cdot l^{g^{q-2}} \cdots l \quad \square$$

*3.2.1. Exhibiting a $p$-complement*

Suppose that $S/L$ is a $p$-complement of $G/L$ exhibited by $\overline{A}$ and that $L$ is an elementary abelian $p$-group. Then $\mathcal{A}$ exhibits $S$ and we want to modify $\mathcal{A}$ such that it exhibits a

$p$-complement of $G$. By Lemma 13, a $p$-complement of $G$ can be obtained as a complement to $L$ in $S$.

Let $(a_{i_1}, \ldots, a_{i_r}, a_{r+1}, \ldots, a_n)$ be the subsequence of $\mathcal{A}$ which forms a pcgs of the exhibited subgroup $S$. We determine elements $l_1, \ldots, l_r$ such that the sequence $\mathcal{B} = (a_{i_1} l_1, \ldots, a_{i_r} l_r)$ is a pcgs of a complement $T$ to $L$ in $S$. Note that a sequence of form $\mathcal{B}$ forms a pcgs for a complement if each power $(a_{i_j} l_j)^{p_{i_j}}$ and each commutator $[a_{i_j} l_j, a_{i_k} l_k]$ is a word in elements of $\mathcal{B}$.

We determine the elements $l_j$ using induction on $j$ from $r$ to 1. Thus suppose that elements $l_{j+1}, \ldots, l_r$ are determined. To shorten the notation we define $b_k = a_{i_k} l_k$, $a = a_{i_j}$ and $q = p_{i_j}$. We consider the power $a^q$ and all commutators $[b_k, a]$ for $k \in \{j+1, \ldots, r\}$. Since $S/L$ is a $p$-complement of $G/L$, we know that $a^q = s \cdot r$ and $[b_k, a] = s_k r_k$ for words $s$ and $s_k$ in $\mathcal{B}$ and elements $r$ and $r_k$ in $L$. Note that $r$ and $r_k$ are just the $p$-parts of the power or commutator. Thus we can use Lemma 15 to determine $l = l_j$ such that $(al)^q = s$ and $[b_k, al] = s_k$ by solving a system of equations over $L$.

*3.2.2. Exhibiting a head complement*

Suppose that $G_{m,2} = 1$ and $L \le G_m$. Let $K/L$ be the complement to $G_m/L$ in $G/L$ exhibited by $\overline{A}$. Then $\mathcal{A}$ exhibits $K$ and we have to adjust $\mathcal{A}$ to $\mathcal{A}'$ so that a complement to $L$ in $K$ is exhibited by $\mathcal{A}'$.

The following method is introduced in Eick and Wright (2002) and we include a brief outline here for completeness. We first characterise the desired complements in a suitable way in the following lemma.

**Lemma 16.** *Let $L$ be an elementary abelian $p$-subgroup of $K$ and let $N \trianglelefteq K$ such that $N/L$ is a nilpotent group and $[L, N] = L$. Let $T$ be a $p$-complement in $N$. Then $N_K(T)$ is a complement to $L$ in $K$.*

We apply Lemma 16 to our situation. Let $N = G_{m-1} \cap K$. Then $N/L \cong G_{m-1}/G_m$ is a nilpotent group and, further, by Theorem 1 we have $[L, N] = L$. Hence $N$ fulfils the requirements of Lemma 16. Further, $N$ is exhibited by $\mathcal{A}$ and thus can be determined easily. We obtain a $p$-complement $T$ of $N$ using the method of Section 3.2.1. Note that a $p$-complement $S/L$ of $N/L$ is exhibited by $\mathcal{A}$ as well and thus we only need to determine a complement to $L$ in $S$.

We adjust $\mathcal{A}$ so that it also exhibits the normaliser $N_K(T)$. Let $g$ be an arbitrary element of $\mathcal{A} \cap K$ and let $t_1, \ldots, t_x$ be generators of $T$. Since $TL \trianglelefteq K$, it follows that $[t_i, g] \in TL$ and thus $[t_i, g] = s_i r_i$ for some $s_i \in T$ and $r_i \in L$. Since $T$ and $L$ have coprime order, $r_i$ is the $p$-part of $[t_i, g]$ and thus is uniquely determined. If $gl \in N_K(T)$, then $[t_i, gl] \in T$ for each $i$. Since $[t_i, gl] \equiv [t_i, g] \bmod L$, it follows that $[t_i, gl] = s_i$ for $1 \le i \le x$ in this case. Hence we get a solution $l \in L$ with $gl \in N_K(T)$ using Lemma 15(a).

## Acknowledgments

The authors thank Alexander Hulpke for reading and commenting on a draft version of this paper. The first author acknowledges the contribution made by John Brownie who identified a number of shortcomings in the original draft of the algorithm while preparing an implementation in Cayley.

## 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., Leedham-Green, C.R., 1990. Special presentations for finite soluble groups (preprint).

Eick, B., 1993. Spezielle PAG-systeme im Computeralgebrasystem GAP. Diplomarbeit, RWTH Aachen.

Eick, B., 1997. Special presentations for finite soluble groups and computing (pre-)Frattini subgroups. In: Finkelstein L., Kantor W.M. (Eds.), Proceedings “Groups and Computation II”. Amer. Math. Soc. DIMACS Series, vol. 28. pp. 101–112 .

Eick, B., Wright, C.R.B., 2002. Computing subgroups by exhibition in finite solvable groups. J. Symbolic Comput. 33, 129–143.

The Gap Group, 2000. GAP—Groups, Algorithms and Programming, 4th edition. www.gap-system.org.

Glasby S.P., 1987. Computational approaches to the theory of finite soluble groups. Ph.D. Thesis, University of Sydney.

Holt, D.F., Leedham-Green, C.R., O’Brien, E.A., Rees, S., 1996. Smash, matrix groups and $G$-Modules, A GAP share package.

Laue, R., Neubüser, J., Schoenwaelder, U., 1984. Algorithms for finite soluble groups and the SOGOS system. In: Proceedings “LMS Symposium on Computational Group Theory”. Academic Press, pp. 105–135.

Leedham-Green, C.R., 1984. A soluble group algorithm. Algorithms for finite soluble groups and the SOGOS system. In: Proceedings “LMS Symposium on Computational Group Theory”. Academic Press, pp. 85–101.

Lux, K., Müller, J., Ringe, M., 1994. Peakword condensation and submodule lattices: an application of the meat-axe. J. Symbolic Comput. 17, 529–544.

Robinson, D.J.S., 1976. The vanishing of certain homology and cohomology groups. J. Pure Appl. Algebra 7, 145–167 .