Formations of Finite Groups in Polynomial Time: \mathfrak{F} -residuals and \mathfrak{F} -subnormality

Viachaslau I. Murashka {mvimath@yandex.ru} Department of Mathematics and Technologies of Programming, Francisk Skorina Gomel State University, Gomel, Belarus

Abstract

For a wide family of formations \mathfrak{F} it is proved that the \mathfrak{F} -residual of a permutation finite group can be computed in a polynomial time. Moreover, if in the previous case \mathfrak{F} is hereditary, then an \mathfrak{F} -subnormality of a subgroup can be checked in a polynomial time.

Keywords. Finite group; permutation group computation; formation; local formation; \mathfrak{F} -subnormality; polynomial time algorithm.

AMS(2010). 20D10, 20B40.

Introduction and the Main Results

All groups considered here are finite. One of the central directions in the modern algebra is the study of different classes of algebraic systems (groups, semigroups, rings, Lie algebras and other). The main problems of it are to construct classes of algebraic systems, to study the structure of a given system in such class and to find wether a given system belongs to a given class or not.

This direction is well illustrated in the rather developed theory of classes of finite groups (formations, Schunk and Fitting classes). The main results in this direction are presented in monographs of Shemetkov [29], Doerk and Hawkes [8], Ballester-Bolinches and Ezquerro [7], Wenbin Guo [11] and others. According to zbMATH Open [1] (formerly known as Zentralblatt MATH) there are more than 5000 papers in this direction (20D10).

The computational theory of classes of finite groups is not as developed as its theoretical part. The main results of this theory are presented in the papers [10] by Eick and Wright and [16] by Höfling and in the corresponding to them GAP packages "FORMAT" [9] and "CRISP" [15] respectively. These papers are dedicated to finding \mathfrak{F} -projectors, \mathfrak{F} -injectors, \mathfrak{F} -residuals and \mathfrak{F} -radicals of soluble groups. Also algorithms for classes of groups where permutability (or one of its generalizations) of subgroups is a transitive relation are studied in the paper [4] by Ballester-Bolinches, Cosme-Llópez and Esteban-Romero and in corresponding to it GAP package "permut" [5]. The principal novelty of this paper is our ability to deal with nonsaturated (non-local) classes of not necessary soluble groups.

A finite group can be defined in the different ways. The most known of them are defining group by presentation, permutations or matrices. One of the main results in the foundation of the theory of formations of finite groups is Sylow's theorems. In [18] Kantor proved that a Sylow subgroup of a permutation group of degree n can be found in polynomial time of n (mod CSFG). So it is natural to ask the following question:

Problem 1. For a given class of groups \mathfrak{X} and a permutation group G of degree n is there a polynomial-type algorithm that checks wether G belongs to \mathfrak{X} ?

That is why we introduce the following definition:

Definition 1. We shall call a class of groups \mathfrak{X} *P*-recognizable if for every $K \leq G \leq S_n$ there is a polynomial-time algorithm that tests wether G/K belongs \mathfrak{X} or not.

Recall that a formation is a class of groups closed under taking homomorphic images and subdirect products. One of the classical ways to study the structure of a group is to find the action of a group on its chief series. For example, formations of nilpotent, supersoluble and quasinilpotent groups; rank [8, VII, Definitions 2.3], local [8, IV, Definitions 3.1], Baer-local [8, IV, Definitions 4.9] and graduated (see [29, §3] or [11, §5.5]) formations are defined by the action of a group on its chief factors. All these formations are particular cases of the following construction.

Definition 2. Let f be a function which assigns 0 or 1 to every group G and its chief factor H/K such that

(1) f(H/K, G) = f(M/N, G) whenever H/K and M/N are G-isomorphic chief factors of G;

(2) f(H/K, G) = f((H/N)/(K/N), G/N) for every $N \leq G$ with $N \leq K$.

Such functions f will be called chief factor functions. Denote by C(f) the class of groups

 $(G \mid f(H/K, G) = 1 \text{ for every chief factor } H/K \text{ of a group group } G).$

For every non-empty formation \mathfrak{F} in every group G there exists the \mathfrak{F} -residual of G, that is the smallest normal subgroup $G^{\mathfrak{F}}$ of G with $G/G^{\mathfrak{F}} \in \mathfrak{F}$. It is clear that $\mathfrak{F} = (G \mid G^{\mathfrak{F}} = 1)$.

Theorem 1. Assume that f(H/K, G) can be computed in polynomial time for every group G and its chief factor H/K. Then $\mathfrak{F} = \mathcal{C}(f)$ is a P-recognizable formation and $G^{\mathfrak{F}}$ can be computed in polynomial time for every $G \leq S_n$.

The concept of subnormality plays an important role in the group's theory. The formational generalization of this concept was introduced in the universe of soluble groups by Hawkes [14] and in the universe of all groups by Shemetkov (see [29, Definition 8.1]). A subgroup H of G is called \mathfrak{F} -subnormal in G, if H = G or there exists a maximal chain of subgroups $H = H_0 \subset H_1 \subset \cdots \subset H_n = G$ such that $H_i/\operatorname{Core}_{H_i}(H_{i-1}) \in \mathfrak{F}$ for $i = 1, \ldots, n$. Note that if \mathfrak{F} is a hereditary formation, then the word "maximal" can be omitted in this definition. Kegel [21] introduced the another such generalization of subnormality. Recall [7, Definition 6.1.4] that a subgroup H of G is called K- \mathfrak{F} -subnormal in G if there is a chain of subgroups $H = H_0 \subseteq H_1 \subseteq \cdots \subseteq H_n = G$ with $H_{i-1} \leq H_i$ or $H_i/\operatorname{Core}_{H_i}(H_{i-1}) \in \mathfrak{F}$ for all $i = 1, \ldots, n$. If $\mathfrak{F} = \mathfrak{N}$, then the notions of K- \mathfrak{F} -subnormal and subnormal subgroups coincide. For more information about \mathfrak{F} -subnormal and K- \mathfrak{F} -subnormal subgroups see [7, Chapter 6].

Theorem 2. Let \mathfrak{F} be a hereditary formation. Assume that $G^{\mathfrak{F}}$ can be computed in polynomial time for every $G \leq S_n$ and natural n. Then there are polynomial-time algorithms that tests wether given subgroup is \mathfrak{F} -subnormal or K- \mathfrak{F} -subnormal.

1 Preliminaries

1.1 Groups and their classes

Recall that M^G denotes the smallest normal subgroup of G which contains M; M' is the derived subgroup of M; M^p is the subgroup generated by p-th powers of elements of M; S_n denotes the symmetric group on n elements; a formation \mathfrak{F} is called hereditary, if $H \leq G \in \mathfrak{F}$ implies $H \in \mathfrak{F}$.

The material of this section can be found, for example, in [8, p. 5-8]. Let Ω be a set. A group G is called an Ω -group if there is associated with each element $\omega \in \Omega$ an endomorphism of G denoted for all $g \in G$ by $g \to g\omega$. A subgroup U of G is called Ω -admissible if $u\omega \in U$ for all $u \in U$ and $\omega \in \Omega$. Evidently the intersection and the join of Ω -admissible subgroups are again Ω -admissible. If N is an Ω -admissible normal subgroup of G, the quotient group G/N may be regarded naturally as an Ω -group via the action defined for all $g \in G$ and $\omega \in \Omega$ by $(Ng)\omega = N(g\omega)$. Finally if G and H are Ω -groups, a isomorphism $\alpha : G \to H$ is called an Ω -isomorphism if for all $g \in G$ and $\omega \in \Omega$ holds $\alpha(g\omega) = \alpha(g)\omega$.

Theorem 3 (The Isomorphism Theorems). Let Ω be a set and let G be an Ω -group.

(1) If U and N are Ω -admissible subgroups of G and U normalizes N, then $UN/N \simeq U/(U \cap N)$ as Ω -groups.

(2) If M and N are Ω -admissible normal subgroups of G and N < M, then the Ω -groups (G/N)/(M/N) and G/M are Ω -isomorphic.

An Ω -group is called Ω -simple if 1 and G are the only Ω -admissible normal subgroups of G. A a subnormal chain $U = U_0, U_1, \ldots, U_n = G$ from U to G is called Ω -series if all of its terms are Ω -admissible. An Ω -series is called Ω -composition series if each factor U_i/U_{i-1} is Ω -simple for $i = 1, \ldots, n$.

Theorem 4 (The Jordan-Hölder Theorem). Let G be an Ω -group, and let

 $1 = N_0 \triangleleft N_1 \triangleleft \cdots \triangleleft N_n = G$ and $1 = M_0 \triangleleft M_1 \triangleleft \cdots \triangleleft M_m = G$

be two Ω -composition series of G. Then m = n and there exists a permutation $\pi \in S_n$ such that for $i = 1, \ldots, n$ the factor N_i/N_{i-1} is Ω -isomorphic with $M_{\pi(i)}/M_{\pi(i)-1}$.

1.2 Computational conventions

Here we use standard computational conventions of abstract finite groups equipped with polynomial-time procedures to compute products and inverses of elements (for the related abstract notion of black-box groups, see [28, Chapter 2]).

Unless stated otherwise, for both input and output, groups are specified by generators. We will consider only $G = \langle S \rangle \leq S_n$ with $|S| \leq n^2$. If necessary, Sims' algorithm [28, Parts 4.1 and 4.2] can be used to arrange that $|S| \leq n^2$.

Quotient groups are specified by generators of a group and its normal subgroup.

According to [2] the following result, all subgroups chains have the bounded length:

Lemma 1 ([2]). Given $G \leq S_n$ every chain of subgroups of G has at most 2n - 3 members for $n \geq 2$.

We need the following well known basis tools in our proves (see, for example [20] or [28]).

Theorem 5. Given $G = \langle S \rangle \leq S_n$, in polynomial time one can solve the following problems:

- 1. Find |G|.
- 2. Given normal subgroups A and B of G, find a composition series for G containing them.
- 3. Given $T \subseteq G$ find $\langle T \rangle^G$.
- 4. (mod CFSG) Given $N, K \leq S_n$ such that N/K is normalized by G/K, find $C_{G/K}(N/K)$ [20, P6(i)].
- 5. (mod CFSG) Given a prime p dividing |G|, find a Sylow p-subgroup P of G and $N_G(P)$ [19].
- 6. Given $H = \langle S_1 \rangle, K = \langle S_2 \rangle \leq G$ find $\langle H, K \rangle = \langle S_1, S_2 \rangle$ and $[H, K] = \langle \{[s_1, s_2] \mid s_1 \in S_1, s_2 \in S_2 \rangle^{\langle H, K \rangle}$.

Lemma 2 ([28, p. 155]). Let H and K be normal subgroups of G such that H/K is an elementary abelian p-group for some prime p. Then H/K can be considered as \mathbb{F}_pG -module. Every generator of G induces by conjugation an linear transformation of this module. Its matrix can be computed in a polynomial time.

2 Proves of the Main Results

2.1 Proof of Theorem 1

The first step is to prove

Lemma 3. If f is a chief factor function, then C(f) is a formation.

Proof. Let $G \in \mathcal{C}(f)$ and $N \leq G$. Then if (H/N)/(K/N) is a chief factor of G/N, then H/K is a chief factor of G and f((H/N)/(K/N), G/N) = f(H/K, G) = 1 by (2) of Definition 2. Hence $G/N \in \mathcal{C}(f)$. It means that $\mathcal{C}(f)$ is closed under taking homomorphic images. Assume now $G/N, G/M \in \mathcal{C}(f)$ and $M \cap N = 1$. Let H/K be a chief factor of G below N. Then

$$HM/KM \simeq H/(H \cap KM) = H/K(H \cap M) = H/K,$$

i.e. H/K is G-isomorphic to a chief factor of G above M by (1) of The Isomorphism Theorems. From the Jordan-Hölder Theorem it follows that every chief factor of G is G-isomorphic to a chief factor of G above M or N. WLOG let $H/K \simeq R/T$ and R/T is a chief factor of G above N, then f(H/K, G) = f(R/T, G) = f((R/N)/(T/N), G/N) = 1 by Definition 2. It means that $G \in C(f)$. Hence C(f) is closed under taking subdirect products. It means that C(f) is a formation.

Recall that the smallest normal subgroup H of G such that G/H is the direct product of simple (resp. simple non-abelian) subgroups of G is called the (resp. non-abelian) residual of Gand is denoted by $\operatorname{Res}(G)$ (resp. $\operatorname{Res}_N(G)$). Here we are interested in the following subgroups. Let M be a normal subgroup of a group G. Denote by $\operatorname{Res}_N(M, G)$ (resp. $\operatorname{Res}_p(M, G)$) the smallest normal subgroup H of G below M such that M/H is the direct product of minimal normal non-abelian (resp. p-subgroups) subgroups of G/H.

Lemma 4. $\operatorname{Res}_N(N,G)$ is defined for every normal subgroup N of G. Moreover $\operatorname{Res}_N(N,G)$ and a decomposition of $N/\operatorname{Res}_N(N,G)$ into the direct product of minimal normal subgroups of $G/\operatorname{Res}_N(N,G)$ can be computed in a polynomial time.

Proof. Note that $\operatorname{Res}_N(N)$ char $N \leq G$. Hence $\operatorname{Res}_N(N) \leq G$. Recall that $\operatorname{Res}_N(N)$ is the smallest normal subgroup of N such that $N/\operatorname{Res}_N(N)$ is a direct product of simple non-abelian groups and every minimal normal non-abelian subgroup is a direct product of simple non-abelian groups. Therefore if $\operatorname{Res}_N(N, G)$ exists, then $\operatorname{Res}_N(N)$ contains it. Let prove that $N/\operatorname{Res}_N(N)$ is the direct product of minimal normal non-abelian subgroups of $G/\operatorname{Res}_N(N)$.

Let A = N and $M/\operatorname{Res}_N(N)$ be a simple subnormal subgroup of $A/\operatorname{Res}_N(N)$. Then $M/\operatorname{Res}_N(N)$ is a simple non-abelian subnormal subgroup of $G/\operatorname{Res}_N(N)$. Therefore $(M/\operatorname{Res}_N(N))^G$ is a minimal normal subgroup of $G/\operatorname{Res}_N(N)$ below $A/\operatorname{Res}_N(N) \leq N/\operatorname{Res}_N(N)$. Note that

$$A/\operatorname{Res}_N(N) = (M/\operatorname{Res}_N(N))^G \times C_{A/\operatorname{Res}_N(N)}((M/\operatorname{Res}_N(N))^G)$$

 $C_{A/\operatorname{Res}_N(N)}((M/\operatorname{Res}_N(N))^G) \leq G/\operatorname{Res}_N(N)$. So now we can let

$$A/\operatorname{Res}_N(N) \leftarrow C_{A/\operatorname{Res}_N(N)}((M/\operatorname{Res}_N(N))^G).$$

It means that using the previous steps we can decompose $N/\text{Res}_N(N)$ into the direct product

of minimal normal non-abelian subgroups of $G/\operatorname{Res}_N(N)$. Thus $\operatorname{Res}_N(N,G) = \operatorname{Res}_N(N)$.

Algorithm	1: NonAbelianDecomposition	(G, N)	
-----------	----------------------------	--------	--

Result: The smallest normal subgroup K of G below N such that $N/K \simeq \overline{N}_1 \times \cdots \times \overline{N}_k$ where \overline{N}_i is a minimal normal non-abelian subgroup of G; subgroups \overline{N}_i . **Data:** N is a normal subgroup of a group G $K \leftarrow Res_N(N)$; $A \leftarrow N$; $L \leftarrow []$; **while** $|A| \neq |K|$ **do** Find a minimal subnormal subgroup B/K of A/K; Find $(B/K)^G$ and add this subgroup to L; $A/K \leftarrow C_{A/K}((B/K)^G)$; **end**

According to [3, Theorem 8.3] $\operatorname{Res}_N(N)$ can be found in polynomial time. By 2 of Theorem 5 the minimal subnormal subgroup $M/\operatorname{Res}_N(N)$ of $N/\operatorname{Res}_N(N)$ can be found in a polynomial time. Then $(M/\operatorname{Res}_N(N))^G = M^G/\operatorname{Res}_N(N)$ can be computed in a polynomial time by 3 of Theorem 5. Now $C_{A/\operatorname{Res}_N(N)}((M/\operatorname{Res}_N(N))^G)$ can be computed in a polynomial time by 4 of Theorem 5. Thus Algorithm 1 runs in a polynomial time by Lemma 1.

Lemma 5. Let p be a prime. $\operatorname{Res}_p(N, G)$ is defined for every normal subgroup N of G. Moreover $\operatorname{Res}_p(N, G)$ and a decomposition of $N/\operatorname{Res}_p(N, G)$ into the direct product of minimal normal subgroups of $G/\operatorname{Res}_p(N, G)$ can be computed in a polynomial time.

Proof. Let N/K be the direct product of minimal normal *p*-subgroups of G/K for a given p where $N, K \leq G$. Note that in this case N/K is the elementary abelian *p*-group. It means that $N'N^p \subseteq K$. So if $N'N^p = N$, then we can let $\operatorname{Res}_p(N,G) = N'N^p$. Assume that $N \neq N'N^p$. Note that $N'N^p$ char $N \leq G$. Hence $N'N^p \leq G$. Then we can consider $V = N/N'N^p$ as an \mathbb{F}_pG -module.

In this case normal subgroups of $G/N'N^p$ below $N/N'N^p$ are in the one to one correspondence with submodules of V. Let $K/N'N^p$ be the radical $\operatorname{Rad}(N/N'N^p)$ of $N/N'N^p$. Now $N/K \simeq (N/N'N^p)/\operatorname{Rad}(N/N'N^p)$ is a semisimple \mathbb{F}_pG -module, i.e. N/K is the direct product of minimal normal subgroups of G/K.

Assume that K_1 is a normal subgroup of G such that $N/K_1 = N_1/K_1 \times \cdots \times N_k/K_1$ is a direct product of minimal normal p-subgroups N_i/K_1 of G/K_1 . It is clear that $N'N^p \subseteq K_1$. Note that $N/(\prod_{i=1,i\neq j}^n N_i)$ is a chief factor of G. It means that $\prod_{i=1,i\neq j}^n N_i/N'N^p$ is a maximal submodule of V. Recall that the radical of a module is the intersection of all its maximal submodules. Now

$$K/N'N^p = \operatorname{Rad}(N/N'N^p) \subseteq \bigcap_{j=1}^n (\prod_{i=1, i \neq j}^n N_i/N'N^p) = K_1/N'N^p.$$

Thus $K \subseteq K_1$. It means that K is the smallest normal subgroup G below N such that N/K is the direct product of minimal normal p-subgroups of G/K. Hence $K = \operatorname{Res}_p(N, G)$ is well defined.

Let show that K can be computed in polynomial time. If $N = \langle S \rangle$, then $N'N^p = \langle \{[x, y] \mid x, y \in S\} \cup \{x^p \mid x \in S\} \rangle$ can be computed in polynomial time. Every generator of G induces by conjugation a linear transformation of $N/N'N^p$. The matrix of this transformation can be found in a polynomial time by Lemma 2. Denote the algebra generated by these matrixes by R. Then the basis of its Jacobson radical J(R) can be computed in a polynomial time by [26, Theorem 2.7]. Now $\operatorname{Rad}(N/N'N^p) = (N/N'N^p)J(R)$ by [8, B, Proposition 4.2]. Hence $\operatorname{Rad}(N/N'N^p)$ is generated (as a module and as a subgroup) by products nr where n is a generator $N/N'N^p$ and r is a generator of J(R). Thus $\operatorname{Rad}(N/N'N^p)$ can be computed in a polynomial time, i.e. $\operatorname{Rad}(N/N'N^p) = K/N'N^p$ and we know generators of K as a subgroup of G.

Since every generator of G induces by conjugation a linear transformation of N/K, the matrix of this transformation can be found in a polynomial time by Lemma 2. Denote the algebra generated by these matrixes by R. Note that N/K is a semisimple \mathbb{F}_pG -module. Hence it is a semisimple R-module. Now nr = 0 for every $n \in N/K$ and $r \in J(R)$. Since R acts on N/K by matrix multiplications, we see that J(R) = 0. Thus R is semisimple. Then bases of minimal ideals R_i of R can be found in polynomial time by [26, Corollary 3.2]. Then $(N/K)R_i$ is a minimal submodule of N/K and the sum of this submodules is N/K by [17, VII, Theorem 12.1]. It is clear that generating sets of these submodules (and hence corresponding to them quotient groups) can be found in a polynomial time.

Algorithm 2: $PDecomposition(G, N, p)$		
Result: The smallest normal subgroup K of G below N such that		
$N/K \simeq \overline{N}_1 \times \cdots \times \overline{N}_k$ where \overline{N}_i is a minimal normal <i>p</i> -subgroup of <i>G</i> ;		
subgroups \overline{N}_i .		
Data: N is a normal subgroup of a group G and p is a prime		
$M \leftarrow [];$		
$L \leftarrow [];$		
$\mathbf{if} \left N^p N' \right = \left N \right \mathbf{then}$		
output $N^p N'$ and L ;		
end		
else		
For each generator g of G find the linear transformation which this element induces on N/N^pN' ;		
For the algebra generated by above mentioned transformations R find the basis of $J(B)$;		
Find the generators of K where $K/N'N^p = (N/N'N^p)J(R)$;		
For each generator g of G find the linear transformation which this element induces on N/K ;		
Decompose the algebra R generated by above mentioned transformations into the sum $\rho_1 \oplus \cdots \oplus \rho_k$ of minimal left ideals;		
For each ideal ρ_i find $(N/K)\rho_i$ and add it to M ;		
For each element in M find its generators in G and add them as an element to L ;		
end		

Lemma 6. Let $\mathfrak{F} = \mathcal{C}(f)$, N and K be normal subgroups of G such that $N/K = N_1/K \times \cdots \times N_t/K$ where N_i/K is a minimal normal subgroup of G and $G/N \in \mathfrak{F}$. Then $(G/K)^{\mathfrak{F}}$ can be found in polynomial time.

Proof. Let

$$I^+ = \{i \mid f(N_i/K, G) = 1\}, I^- = \{i \mid f(N_i/K, G) = 0\} \text{ and } M/K = \prod_{i \in I^-} N_i/K.$$

We claim that $M/K = (G/K)^{\mathfrak{F}}$. Note that every chief factor H/T of G between M and N is G-isomorphic to N_i/K for some $i \in I^+$. Hence

$$f((H/M)/(T/M), G/M) = f(H/T, G) = f(N_i/K, G) = 1.$$

Since $G/N \simeq (G/M)/(N/M) \in \mathcal{C}(\mathbf{f})$, we see that f((H/M)/(T/M), G/M) = 1 for every chief factor (H/M)/(T/M) of G/M above N/M. From the Jordan-Hölder theorem it follows that $(G/K)/(M/K) \simeq G/M \in \mathcal{C}(\mathbf{f}) = \mathfrak{F}$. Hence $(G/K)^{\mathfrak{F}} \leq M/K$.

Assume that $F/K = (G/K)^{\mathfrak{F}} < M/K$. So $I^- \neq \emptyset$. Then $F/K < FN_i/K$ for some $i \in I^-$, i.e. $F \cap N_i = K$. Hence FN_i/F and N_i/K are G-isomorphic chief factors of G. Thus

$$1 = f(((FN_i/K)/(F/K))/((F/K)), (G/K)/(F/K)) = f((FN_i/K)/(F/K), G/K) = f(FN_i/F, G) = f(N_i/K, G) = 0,$$

a contradiction. Thus $(G/K)^{\mathfrak{F}} = M/K$. Algorithm 3: FResidualPart(G, N, K, L, f)Result: $T/K = (G/K)^{\mathfrak{F}}$. Data: $N \trianglelefteq G$ with $G/N \in \mathfrak{F}, K \trianglelefteq G$ with $N/K = N_1/K \times \cdots \times N_t/K$; the list L of minimal normal subgroups N_i/K of G/K. $T \leftarrow K$; for i in [1, ..., t] do $| if f(N_i/K, G) = 0$ then $| T \leftarrow \langle T, N_i \rangle$ end end

Since f(H/K, G) can be computed in a polynomial time for every chief factor H/K of G, we see that I^- can be computed in a polynomial time. Note that t < 2n by Lemma 1. Hence the join of not more than t subgroups can be computed in a polynomial time.

Lemma 7. Let $\mathfrak{F} = \mathcal{C}(f)$ and G be a group. Then $G^{\mathfrak{F}}$ can be computed in a polynomial time.

Proof. Note that $G/G \in \mathcal{C}(f)$. Assume that we have a subgroup H with $G/H \in \mathcal{C}(f)$. Then $G^{\mathfrak{F}} \subseteq H$. If $G^{\mathfrak{F}} \neq H$, then there is a chief factor H/K of G with f(H/K, G) = 1. Note that H/K is either a non-abelian or an abelian p-group. Hence H/K is G-isomorphic to a chief factor of G between $\operatorname{Res}_N(H, G)$ and H or between $\operatorname{Res}_p(H, G)$ and H for some p.

Algorithm 4: FResidual(G, f)

Result: $N = G^{\mathfrak{F}}$. Data: $\mathfrak{F} = \mathcal{C}(f)$, G is a group. $K \leftarrow G$; repeat $N \leftarrow K$; $K \leftarrow \text{FResidualPart}(G, K, \text{NonAbelianDecomposition}(G, K), f)$; $\pi \leftarrow \pi(K)$; for p in π do $\mid K \leftarrow \text{FResidualPart}(G, K, \text{PDecomposition}(G, K, p), f)$; end until $|N| \neq |K|$;

From Lemmas 4–7 it follows that this is a polynomial time algorithm.

Lemma 8. Let $\mathfrak{F} = \mathcal{C}(f)$. Then \mathfrak{F} is *P*-recognizable.

Proof. Let G be a group. Then $G^{\mathfrak{F}}$ can be computed in a polynomial time. Recall that $(G/K)^{\mathfrak{F}} = G^{\mathfrak{F}}K/K$. Hence $G/K \in \mathfrak{F}$ iff $G^{\mathfrak{F}} \subseteq K$ iff $\langle G^{\mathfrak{F}}, K \rangle = K$ iff $|\langle G^{\mathfrak{F}}, K \rangle| = |K|$. The last condition can be checked in polynomial time by 1 and 6 of Theorem 5.

3 Proof of Theorem 2

Let H be a K- \mathfrak{F} -subnormal subgroup of G. From the definition of K- \mathfrak{F} -subnormal subgroup it follows that either G = H or there is a proper subgroup M of G with H is a K- \mathfrak{F} -subnormal subgroup of M and $M \leq G$ or $G^{\mathfrak{F}} \leq M$.

Algorithm 5: ISKFSUBNORMAL (G, H, \mathfrak{F})

```
Result: True if H is K-\mathfrak{F}-subnormal in G and False otherwise.

Data: A subgroup H of a group G.

if |G| = |H| then

| return True;

else

| if |HG^{\mathfrak{F}}| \neq |G| then

| return ISKFSUBNORMAL(HG^{\mathfrak{F}}, H, \mathfrak{F});

else

| if |H^G| \neq |G| then

| return ISKFSUBNORMAL(H^G, H, \mathfrak{F});

| end

end

return False;

end
```

Since $G^{\mathfrak{F}}$ can be computed in a polynomial time and according to 1 and 3 of Theorem 5, we see that every above mentioned check can be made in a polynomial time. Now the statement of theorem follows from the fact that every chain of subgroups of G has at most 2n members by Lemma 1.

By analogy one can prove that the following algorithm tests $\mathfrak{F}\text{-subnormality}$ in a polynomial time.

Algorithm 6: ISFSUBNORMAL (G, H, \mathfrak{F})

```
Result: True if H is \mathfrak{F}-subnormal in G and False otherwise.

Data: A subgroup H of a group G.

if |G| = |H| then

| return True;

else

| if |HG^{\mathfrak{F}}| \neq |G| then

| return ISFSUBNORMAL(HG^{\mathfrak{F}}, H, \mathfrak{F});

else

| return False;

end

end
```

4 Applications

4.1 Local and Baer-local formations

Recall [8, IV, Definitions 3.1] that a function f which assigns a formation to each prime is called a *formation function*; a chief factor H/K of a group G is called *f*-central if $G/C_G(H/K) \in f(p)$ for all prime divisors of |H/K|; a formation \mathfrak{F} is called *local* if its coincides with the class of groups all whose chief factors are *f*-central for some formation function f. In this case f is called a local definition of \mathfrak{F} . **Theorem 6.** Let $f_{\mathfrak{F}}$ be a local definition of a local formation \mathfrak{F} . Assume that $G^{f_{\mathfrak{F}}(p)}$ can be computed in a polynomial time for every prime p and every group G. Then \mathfrak{F} is P-recognizable and $G^{\mathfrak{F}}$ can be computed in a polynomial time.

Proof. Note that

$$G/C_G(H/K) \in f_{\mathfrak{F}}(p) \qquad \forall p \in \pi(H/K)$$

$$\Leftrightarrow G^{f_{\mathfrak{F}}(p)} \subseteq C_G(H/K) \qquad \forall p \in \pi(H/K)$$

$$\Leftrightarrow [G^{f_{\mathfrak{F}}(p)}, H] \subseteq K \qquad \forall p \in \pi(H/K)$$

$$\Leftrightarrow |\langle [G^{f_{\mathfrak{F}}(p)}, H], K \rangle| = |K| \quad \forall p \in \pi(H/K).$$

Let

$$f_{\mathfrak{F}}(H/K,G) = \begin{cases} 1, & H/K \text{ is } f_{\mathfrak{F}}\text{-central}; \\ 0, & \text{otherwise.} \end{cases} = \begin{cases} 1, & |\langle [G^{f_{\mathfrak{F}}(p)}, H], K \rangle| = |K| \quad \forall p \in \pi(H/K); \\ 0, & \text{otherwise.} \end{cases}$$

From the definition of local formation it follows that $\mathfrak{F} = \mathcal{C}(\mathbf{f}_{\mathfrak{F}})$. Since $G^{f_{\mathfrak{F}}(p)}$, the commutator of two subgroups, the join of two subgroups and the order of subgroup can be computed in a polynomial time, we see that $f_{\mathfrak{F}}(H/K, G)$ can be computed in a polynomial time.

Lets prove that $f_{\mathfrak{F}}$ is a chief factor function. If H/K and M/N are G-isomorphic chief factors, then $C_G(H/K) = C_G(M/N)$. Hence $G/C_G(H/K) = G/C_G(M/N)$. Therefore $f_{\mathfrak{F}}$ satisfies (1) of Definition 2. Note that if $[G^{f_{\mathfrak{F}}(p)}, H] \subseteq K$ for all $p \in \pi(H/K)$, then

$$[(G/N)^{f_{\mathfrak{F}}(p)}, H/N] = [G^{f_{\mathfrak{F}}(p)}N/N, H/N] = [G^{f_{\mathfrak{F}}(p)}, H]N/N \subseteq K/N \quad \forall p \in \pi((H/N)/(K/N)).$$

Hence $f_{\mathfrak{F}}$ satisfies (2) of Definition 2.

Therefore the statement of Theorem 6 directly follows from Theorem 1.

The following classes of groups are local formations:

- 1. The class \mathfrak{U} of all supersoluble groups. It is locally defined by $f_{\mathfrak{U}}(p) = \mathfrak{A}(p-1)$ (the class of all abelian groups of exponent dividing p-1).
- 2. The class $w\mathfrak{U}$ of widely supersoluble groups [30]. It is locally defined by $f_{w\mathfrak{U}}(p) = \mathcal{A}(p-1)$ (the class of all groups all whose Sylow subgroups are abelian of exponent dividing p-1).
- 3. The class $\mathfrak{N}\mathcal{A}$ of groups G such that all Sylow subgroups of G/F(G) are abelian [30]. It is locally defined by $f_{\mathfrak{N}\mathcal{A}}(p) = \mathcal{A}$ (the class of groups all whose Sylow subgroups are abelian).
- 4. In [33] the class $sm\mathfrak{U}$ of groups with submodular Sylow subgroups were studied. It is locally defined [32] by $f_{sm\mathfrak{U}}(p) = \mathcal{A}(p-1) \cap \mathfrak{B}$ where \mathfrak{B} is a class of groups with square-free exponent.
- 5. The class of strongly supersoluble groups $s\mathfrak{U}$ [32]. Its local definition $f_{\mathfrak{s}\mathfrak{U}}(p) = \mathfrak{A}(p-1) \cap \mathfrak{B}$.
- 6. The class $sh\mathfrak{U}$ of groups all whose Schmidt subgroups are supersoluble [22, 23]. Its local definition $f_{sh\mathfrak{U}}(p) = \mathfrak{G}_{\pi(p-1)}$ (the class of all $\pi(p-1)$ -groups).

Corollary 1. Let $\mathfrak{F} \in {\mathfrak{U}, \mathfrak{wl}, \mathfrak{sl}, \mathfrak{sml}, \mathfrak{NA}, \mathfrak{shl}}$. Then \mathfrak{F} is *P*-recognizable and $G^{\mathfrak{F}}$ can be computed in a polynomial type. In particular, \mathfrak{F} -subnormality of a subgroup can be tested in a polynomial time.

Proof. Let $G = \langle S \rangle$. Note that the generating set S_p of a Sylow p-subgroup of G can be computed in a polynomial time by 4 of Theorem 5. It is straightforward to check that

- $\begin{array}{l} 1. \ G^{f_{\mathfrak{U}}(p)} = \langle \{[x,y], x^{p-1} \mid x,y \in S\} \rangle. \\ 2. \ G^{f_{w\mathfrak{U}}(p)} = \langle (\bigcup_{p \in \pi(G)} \{[x,y], x^{p-1} \mid x,y \in S_p\})^G \rangle. \end{array}$
- 3. $G^{f_{\mathfrak{N}\mathcal{A}}(p)} = \langle (\bigcup_{p \in \pi(G)} \{ [x, y] \mid x, y \in S_p \})^G \rangle.$
- 4. $G^{f_{sm\mathfrak{U}}(p)} = \langle (\bigcup_{p \in \pi(G)} \{ [x, y], x^{\prod_{q \in \pi(p-1)} q} \mid x, y \in S_p \})^G \rangle.$
- 5. $G^{f_{\mathfrak{sll}}(p)} = \langle \{ [x, y], x^{\prod_{q \in \pi(p-1)} q} \mid x, y \in S \} \rangle.$
- 6. $G^{f_{shu}(p)} = \langle (\bigcup_{p \notin \pi(p-1)} \{ x \mid x \in S_p \})^G \rangle.$

Hence every of the above mentioned subgroups can be computed in a polynomial time. Note that all these formations are hereditary. Thus the statement of a corollary directly follows from Theorems 2 and 6.

Let f be a local definition of a local formation \mathfrak{F} . Recall that if $f(p) \subseteq \mathfrak{F}$ for all p, then every f-central chief factor is called \mathfrak{F} -central and every non-f-central chief factor is called *S*-eccentric.

Lemma 9. Assume that $f_{\mathfrak{F}}$ is a local definition of a local formation \mathfrak{F} and $G^{f_{\mathfrak{F}}(p)}$ can be computed in a polynomial time for every prime $p \in \pi(G)$. Then $G^{F_{\mathfrak{F}}(p)}$ can be computed in a polynomial time for every prime $p \in \pi(G)$ where $F_{\mathfrak{F}}$ is the canonical local definition of \mathfrak{F} . In particular the check of \mathfrak{F} -centrality of a chief factor can be done in a polynomial time.

Proof. Recall that $F_{\mathfrak{F}}(p) = \mathfrak{N}_p(\mathfrak{F} \cap f_{\mathfrak{F}}(p))$. So $G^{F_{\mathfrak{F}}(p)} = (G^{f_{\mathfrak{F}}(p)}G^{\mathfrak{F}})^{\mathfrak{N}_p}$ can be computed in a polynomial time by Theorem 6 for any $p \in \pi(G)$. Following the proof of this theorem we can check a chief factor for $F_{\mathfrak{F}}$ -centrality (which is the same as \mathfrak{F} -centrality) in a polynomial time.

One of important families of formations are Baer-local or composition formations. There are many ways to define them (see [8, IV, Definitions 4.9], [11, p. 4] and [29, Definition 3.11]). A function of the form $f: \{Simple groups\} \to \{formations\}$ is called a Baer function. $f(Z_p)$ is denoted by f(p) where Z_p is a cyclic group of order p. A chief factor H/K of a group G is called f-central if $G/C_G(H/K) \in f(S)$ where all composition factors of H/K are isomorphic to S. A formation \mathfrak{F} is called *Baer-local* if its coincides with the class of groups all whose chief factors are f-central for some Baer function f. It is known (see [11, 1, Theorem 1.6]) that Baer-local formation can be defined by Baer function f such that f(0) = f(S) for every non-abelian simple group.

Theorem 7. Let f be a Baer-local definition of a composition formation \mathfrak{F} . Assume that $G^{f(x)}$ can be computed in polynomial time for every $x \in \mathbb{P} \cup \{0\}$. Then \mathfrak{F} is P-recognizable and $G^{\mathfrak{F}}$ can be computed in polynomial time.

Proof. Let

$$f_{\mathfrak{F}}(H/K,G) = \begin{cases} 1, & H/K \text{ is non-abelian and } |\langle [G^{f_{\mathfrak{F}}(0)}, H], K \rangle| = |K|; \\ 1, & H/K \text{ is a } p\text{-group and } |\langle [G^{f_{\mathfrak{F}}(p)}, H], K \rangle| = |K|; \\ 0, & \text{otherwise.} \end{cases}$$

As in the proof of Theorem 6 we can chow that $f_{\mathfrak{F}}$ is a chief factor function and $\mathfrak{F} = \mathcal{C}(f_{\mathfrak{F}})$. \Box

4.2The lattice of chief factor functions

For a chief factor functions f_1 and f_2 let

1. $(f_1 \vee f_2)(H/K, G) = 1$ iff $f_1(H/K, G) = 1$ or $f_2(H/K, G) = 1$.

- 2. $(f_1 \wedge f_2)(H/K, G) = 1$ iff $f_1(H/K, G) = 1$ and $f_2(H/K, G) = 1$.
- 3. $\overline{f}_1(H/K, G) = 1$ iff $f_1(H/K, G) = 0$.

It is straightforward to check that these functions are chief factor functions. If $f_1(H/K, G)$ and $f_2(H/K, G)$ can be computed in a polynomial time, then functions from 1–3 can also be computed in a polynomial time. Note that the first two items defines the structure of a distributive lattice on the set of chief factor functions.

Theorem 8. *P*-recognizable chief factor formations form a distributive lattice.

The formation \mathfrak{F} of groups whose 3-chief factors are not central plays an important role as a counterexample in the study of mutual permutable products of groups (see [6, Example 4.4.8]). It is clear that this class of groups is defined by a chief factor function f such that f(H/K, G) = 1 if H/K is not a central 3-chief factor or is not a 3-chief factor. Since the orders of a chief factor and its centralizer can be computed in a polynomial time by Theorem 5, we see

Proposition 1. The formation of groups whose 3-chief factors are not central is P-recognizable.

It is well known that any Baer-local formation \mathfrak{F} can be defined by Baer-function $F_{\mathfrak{F}}$ such that $F_{\mathfrak{F}}(0) = \mathfrak{F}$, i.e. the general definition of Baer-local formation gives little information about the action of an \mathfrak{F} -group G on its non-abelian chief factors. Therefore several families of Baer-local formations were introduced by giving additional information about the action of an \mathfrak{F} -group on its non-abelian chief factors. For example, in [12, 13] Guo and Skiba introduced the class \mathfrak{F}^* of quasi- \mathfrak{F} -groups for a saturated formation \mathfrak{F} :

 $\mathfrak{F}^* = (G \mid \text{for every } \mathfrak{F}\text{-eccentric chief factor } H/K \text{ and every } x \in G, x \text{ induces an inner automorphism on } H/K).$

If $\mathfrak{N} \subseteq \mathfrak{F}$ is a normally hereditary local formation, then \mathfrak{F}^* is a normally hereditary Baer-local formation by [12, Theorem 2.6].

Theorem 9. Let $f_{\mathfrak{F}}$ be a local definition of a local formation \mathfrak{F} . Assume that $G^{f_{\mathfrak{F}}(p)}$ can be computed in a polynomial time for every prime p. Then \mathfrak{F}^* is P-recognizable and $G^{\mathfrak{F}^*}$ can be computed in a polynomial time.

Proof. Note that every element of a group G induces an inner automorphism on a chief factor H/K if and only if $HC_G(H/K) = G$. The last condition can be checked in a polynomial time by Theorem 5. Now we can check that either a chief factor is \mathfrak{F} -central or every element of a group G induces an inner automorphism on it in a polynomial time by Lemma 9. Thus \mathfrak{F}^* is P-recognizable and $G^{\mathfrak{F}^*}$ can be computed in a polynomial time by Theorem 1.

Corollary 2. Formation \mathfrak{N}^* of all quasinilpotent groups is *P*-recognizable and $G^{\mathfrak{N}^*}$ can be computed in a polynomial time.

4.3 *§*-subnormal subgroups

In [24, 25, 27, 31] groups with K- \mathfrak{F} -subnormal or \mathfrak{F} -subnormal Sylow subgroups were studied. The class of all groups with K- \mathfrak{F} -subnormal (resp. \mathfrak{F} -subnormal) Sylow π -subgroups was denoted by $\overline{w}_{\pi}\mathfrak{F}$ (resp. $w_{\pi}\mathfrak{F}$, see [31]).

Theorem 10. Let \mathfrak{F} be a hereditary formation such that $G^{\mathfrak{F}}$ can be computed in a polynomial time for every group G and π be a set of primes such that $\pi(G) \cap \pi$ can be computed in polynomial time for every group G. Then $w_{\pi}\mathfrak{F}$ and $\overline{w}_{\pi}\mathfrak{F}$ are P-recognizable formations.

Proof. Note that if a Sylow p-subgroup of G is K- \mathfrak{F} -subnormal, then every Sylow p-subgroup of every quotient group of G is K- \mathfrak{F} -subnormal in it. Assume now that P is not a K- \mathfrak{F} subnormal Sylow subgroup of G. Then ISKFSUBNORMAL (G, P, \mathfrak{F}) finds a K- \mathfrak{F} -subnormal in G subgroup M = M(P) of G with $P^M = M$ and $PM^{\mathfrak{F}} = M$. Assume that a Sylow p-subgroup PN/N is K- \mathfrak{F} -subnormal in G/N. Since \mathfrak{F} is a hereditary formation, we see that PN/N is K- \mathfrak{F} -subnormal in MN/N. From $(PN/N)^{MN/N} = P^M N/N = MN/N$ and $(PN/N)(M/N)^{\mathfrak{F}} = (PN/N)(M^{\mathfrak{F}}N/N) = MN/N$ it follows that PN/N = MN/N is a p-group. Hence $O^p(M) \leq N$. From the other hand M is K \mathfrak{F} subnormal in G hence if $O^p(M) \leq N$ then PN/N = N/N

From the other hand M is K- \mathfrak{F} -subnormal in G. Hence if $O^p(M) \leq N$, then PN/N = MN/N is a K- \mathfrak{F} -subnormal Sylow p-subgroup of G/N.

Thus $G^{\overline{w}\pi\mathfrak{F}}$ is a normal closure of a subgroup generated by $O^p(M(P))$ where P is a non-K- \mathfrak{F} -subnormal subgroup of G for $p \in \pi$. From Theorem 5 it follows that this subgroup can be computed in a polynomial time.

The algorithm for computing $G^{\mathbf{w}_{\pi}\mathfrak{F}}$ uses the same ideas.

Acknowledgments

I am grateful to A.F. Vasil'ev for helpful discussions.

References

- [1] Papers with classification 20D10, Feb. 2021.
- [2] L. BABAI, On the length of subgroup chains in the symmetric group, Comm. Algebra, 14 (1986), pp. 1729–1736.
- [3] L. BABAI, E. M. LUKS, AND A. SERESS, Permutations Groups in NC, in Proc. 19th ACM STOC, 1987, pp. 409–420.
- [4] A. BALLESTER-BOLINCHES, E. COSME-LLÖPEZ, AND R. ESTEBAN-ROMERO, Algorithms for permutability in finite groups, Cent. Eur. J. Math., 11 (2013), pp. 1914–1922.
- [5] ____, GAP package permut A package to deal with permutability in finite groups, v. 2.0.3, 2018, 2014.
- [6] A. BALLESTER-BOLINCHES, R. ESTEBAN-ROMERO, AND M. ASAAD, *Products of Finite Groups*, De Gruyter, 2010.
- [7] A. BALLESTER-BOLLINCHES AND L. M. EZQUERRO, *Classes of Finite Groups*, vol. 584 of Math. Appl., Springer Netherlands, 2006.
- [8] K. DOERK AND T. O. HAWKES, *Finite Soluble Groups*, vol. 4 of De Gruyter Exp. Math., De Gruyter, Berlin, New York, 1992.
- [9] B. EICK AND C. R. WRIGHT, GAP package FORMAT Computing with formations of finite solvable groups, v.1.4.3, 2020, 2000.
- [10] , Computing Subgroups by Exhibition in Finite Solvable Groups, J. Symb. Comput., 33 (2002), pp. 129–143.
- [11] W. GUO, Structure Theory for Canonical Classes of Finite Groups, Springer-Verlag, Berlin, Heidelberg, 2015.
- [12] W. GUO AND A. N. SKIBA, On Finite Quasi-F-Groups, Comm. Algebra, 37 (2009), pp. 470–481.
- [13] —, On some classes of finite quasi-*F*-groups, J. Group Theory, 12 (2009), pp. 407–417.

- [14] T. HAWKES, On Formation Subgroups of a Finite Soluble Group, J. London Math. Soc., s1-44 (1969), pp. 243–250.
- [15] B. HöFLING, GAP package CRISP Computing with Radicals, Injectors, Schunck classes and Projectors, v. 1.4.5, 2019, 2000.
- [16] —, Computing Projectors, Injectors, Residuals and Radicals of Finite Soluble Groups, J. Symb. Comput., 32 (2001), pp. 499–511.
- [17] B. HUPPERT AND N. BLACKBURN, *Finite Groups II*, Grundlehren der mathematischen Wissenschaften, Springer, Berlin, Heidelberg, 1982.
- [18] W. M. KANTOR, Sylow's theorem in polynomial time, J. Comput. Syst. Sci., 30 (1985), pp. 359– 394.
- [19] —, Finding Sylow normalizers in polynomial time, J. Algorithms, 11 (1990), pp. 523–563.
- [20] W. M. KANTOR AND E. M. LUKS, Computing in quotient groups, in Proceedings of the Twenty– Second Annual ACM Symposium on Theory of Computing, Baltimore, May 14–16, New York, 1990, ACM, pp. 524–534.
- [21] O. H. KEGEL, Untergruppenverbände endlicher Gruppen, die den Subnormalteilerverband echt enthalten, Arch. Math., 30 (1978), pp. 225–228.
- [22] V. S. MONAKHOV, Finite groups with a given set of Schmidt subgroups, Math. Notes, 58 (1995), pp. 1183–1186.
- [23] , *Three Formations over* \mathfrak{U} , Math. Notes, 110 (2021), pp. 339–346.
- [24] V. S. MONAKHOV AND I. L. SOKHOR, On groups with formational subnormal Sylow subgroups, J. Group Theory, 21 (2018), pp. 273–287.
- [25] V. I. MURASHKA, Finite groups with given sets of *S*-subnormal subgroups, Asian-European J. Math., 13 (2018), p. 2050073.
- [26] L. RÓNYAI, Computing the structure of finite algebras, J. Symb. Comput., 9 (1990), pp. 355–373.
- [27] V. N. SEMENCHUK AND S. N. SHEVCHUK, Characterization of classes of finite groups with the use of generalized subnormal Sylow subgroups, Math. Notes, 89 (2011), pp. 117–120.
- [28] A. SERESS, Permutation Group Algorithms, Cambridge University Press, Cambridge, 2003.
- [29] L. A. SHEMETKOV, Formations of finite groups, Nauka, Moscow, 1978. In Russian.
- [30] A. F. VASIL'EV, T. I. VASIL'EVA, AND V. N. TYUTYANOV, On the finite groups of supersoluble type, Sib. Math. J., 51 (2010), pp. 1004–1012.
- [31] A. F. VASIL'EV, T. I. VASIL'EVA, AND A. S. VEGERA, Finite groups with generalized subnormal embedding of Sylow subgroups, Sib. Math. J., 57 (2016), pp. 200–212.
- [32] V. A. VASILYEV, Finite groups with submodular sylow subgroups, Sib. Math. J., 56 (2015), pp. 1019–1027.
- [33] I. ZIMMERMANN, Submodular subgroups in finite groups, Math. Z., 202 (1989), pp. 545–557.