J. Group Theory **8** (2005), 171–188

Journal of Group Theory

The X-Dirichlet polynomial of a finite group

Andrea Lucchini

(Communicated by J. S. Wilson)

1 Introduction

Suppose that G is a finite group and fix a subset X of G. For any positive integer t, let $\phi_G(X,t)$ denote the number of ordered t-tuples $(g_1,\dots,g_t)$ of group elements such that $G=\langle X,g_1,\dots,g_t\rangle$. The number $P_G(X,t)=\phi_G(X,t)/|G|^t$ is the probability that t randomly chosen elements generate G together with the elements of the subset X. Clearly $\sum_{X\subseteq H\leqslant G}\phi_H(X,t)=|G|^t$; applying the Möbius inversion formula we obtain

$$\phi_G(X,t)=\sum_{X\subseteq H\leqslant G}\mu(H,G)|H|^t, \tag{1.1}$$

where μ is the Möbius function associated with the subgroup lattice of G. In view of (1.1), we may write

$$P_G(X,t)=\sum_{X\subseteq H\leqslant G}\frac{\mu(H,G)}{|G:H|^t}. \tag{1.2}$$

We may interpolate the above integer function and define $P_G(X,s)$ for any complex variable s. Rearranging the summands in (1.2) we obtain a Dirichlet polynomial as follows:

$$P_G(X,s):=\sum_{n\in\mathbb{N}}\frac{a_n}{n^s}\quad\text{where } a_n:=\sum_{\substack{|G:H|=n,\\ X\subseteq H\leqslant G}}\mu(H,G).$$

The formula (1.2) when $X=\varnothing$ was discovered by Hall [7]; in this case $P_G(\varnothing,s)$ is the multiplicative inverse of a zeta function for G, as described by Mann [9] and Boston [2].

The ring $\mathscr{D}$ of Dirichlet polynomials with integer coefficients is a unique factorization domain. In [5] it is shown that if $X = \varnothing$ then knowledge of the chief factors of G gives a factorization of $P_G(X,s)$ in $\mathscr{D}$. Our aim here is to prove similar results for arbitrary choices of X. The starting remark is that normal subgroups play a crucial role in the factorization of $P_G(X,s)$. Indeed (see Proposition 16) if $N \trianglelefteq G$, then there exists a polynomial $P_{G,N}(X,t) \in \mathscr{D}$ such that

$$P_G(X,s) = P_{G/N}(XN,s)P_{G,N}(X,s). \tag{1.3}$$

By taking a chief series of G, and iterating the above formula, we obtain an expression of $P_G(X,s)$ as a product indexed by the factors of the series. As in the case $X = \varnothing$, the main result is that *the factors of $P_G(X,s)$ obtained in this way are independent of the choice of the chief series*. We shall describe the Dirichlet polynomials that arise in this kind of factorization. A key tool in the case when $X = \varnothing$ was an equivalence relation on the set of irreducible G-groups. Here we refine this equivalence relation, to take account of the behaviour of the irreducible G-groups with respect to the subset X. We place the results of [5], [8] in this more general setting. Though in some cases the modifications required are slight, we have included them in order to make our exposition self-contained.

2 (G,X)-equivalence and crowns

Throughout this paper, G denotes a finite group and X is a subset of G.

Definition 1. Let A and B be two G-groups. We say that they are (G,X)-*equivalent*, and write $A \sim_{G,X} B$, if there are isomorphisms $\phi : A \to B$ and $\Phi : A \rtimes G \to B \rtimes G$ such that

(1) $x^{\Phi} = x$ for all $x \in X$, and

(2) the following diagram commutes:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & A & \longrightarrow & A \rtimes G & \longrightarrow & G & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \Phi} & & \| & & \\ 1 & \longrightarrow & B & \longrightarrow & B \rtimes G & \longrightarrow & G & \longrightarrow & 1. \end{array}$$

This relation is an equivalence relation and it was studied by Jiménez-Seral and Lafuente [8] when $X = \varnothing$. In this particular case we write $A \sim_G B$ instead of $A \sim_{G,X} B$ and we say that A and B are G-equivalent. Clearly if $A \sim_{G,X} B$, then $A \sim_G B$, but, as we will see, (G,X)-equivalence is in general strictly weaker than G-equivalence. However most of the results proved in [8] concerning G-equivalence can be generalized to (G,X)-equivalence.

Arguing as in [8, Proposition 1.2], we can translate our definition of (G,X)-equivalence in terms of non-abelian cohomology. Given a G-group B and a 1-cocycle

$\beta \in \mathrm{Z}^1(G,B)$, we get that $b^{g^\eta} = b^{gg^\beta}$ defines a homomorphism $\eta : G \to \mathrm{Aut}\, B$. The corresponding G-group is denoted by B_β. We write

$$\mathrm{Z}^1_X(G,B) = \{\beta \in \mathrm{Z}^1(G,B) \mid x^\beta = 1 \text{ for all } x \in X\}.$$

Proposition 2. *Let A and B be two G-groups. Then $A \sim_{G,X} B$ if and only if there exists $\beta \in \mathrm{Z}^1_X(G,B)$ such that $A \cong_G B_\beta$.*

Proof. Given $\beta \in \mathrm{Z}^1_X(G,B)$ and an isomorphism $\phi : A \to B$ such that $a^{g\phi} = a^{\phi g g^\beta}$ for all $a \in A$, $g \in G$, we may define $\Phi : A \rtimes G \to B \rtimes G$ by $(ga)^\Phi = gg^\beta a^\phi$ and obtain $A \sim_{G,X} B$. On the other hand if $A \sim_{G,X} B$, then we may define $\beta : G \to B$ by $g^\beta = g^{-1} g^\Phi$. The result follows.

A consequence of the previous proposition is that if $A \cong_G B$, then $A \sim_{G,X} B$, independently of the choice of X (indeed we can take $\beta \in \mathrm{Z}^1(G,B)$ such that $g^\beta = 1$ for all $g \in G$). Moreover, if A and B are abelian, then $B_\beta = B$ for any $\beta \in \mathrm{Z}^1_X(G,B)$, and hence if $A \sim_{G,X} B$, then $A \cong_G B$. Therefore two abelian G-groups are (G,X)-equivalent if and only if they are G-isomorphic. However in the non-abelian case the (G,X)-equivalence relation depends on the choice of the subset X, as illustrated in the following example:

Example 3. Take a non-abelian simple group S and let $G = S^2$. The minimal normal subgroups $S_1 = \{(s,1) \mid s \in S\}$ and $S_2 = \{(1,s) \mid s \in S\}$ are irreducible G-groups. Define $\beta \in \mathrm{Z}^1(G, S_2)$ by setting $(a,b)^\beta = (1, b^{-1}a)$. Then $S_1 \cong_G (S_2)_\beta$ since the map $\phi : S_1 \to S_2$ defined by $(s,1)^\phi = (1,s)$ satisfies the condition $a^{g\phi} = a^{\phi g g^\beta}$ for any $a \in S_1$, $g \in G$; hence if $X \subseteq \{(s,s) \mid s \in S\}$, then $\beta \in \mathrm{Z}^1_X(G, S_2)$ and $S_1 \sim_{G,X} S_2$. However if $X = S_2$, then S_1 and S_2 are not (G,X)-equivalent. Otherwise there would exist $\beta \in \mathrm{Z}^1_{S_2}(G, S_2)$ such that $S_1 \cong_G (S_2)_\beta$, but in this case $g^\beta = 1$ for all $g \in G$, and $S_1 \sim_{G,S_2} S_2$ would imply that $S_1 \cong_G S_2$, which is false since $C_G(S_1) \neq C_G(S_2)$.

Note that a G-group B which is (G,X)-equivalent to an irreducible G-group A is not necessarily irreducible; indeed consider the following example:

Example 4. Let S be a non-abelian simple group and let T be a subgroup of S. Consider the direct product $G = S \times T$ and let $X = \{(t,t) \mid t \in T\}$. Define actions $\alpha_i : G \to \mathrm{Aut}\, S$ for $i = 1, 2$ in the following way:

$$x^{(s,t)^{\alpha_1}} = x^s, \quad x^{(s,t)^{\alpha_2}} = x^t \quad \text{for any } x \in S,\ (s,t) \in G.$$

Denote by S_1 and S_2 the G-groups corresponding to these two actions. Define $\beta : G \to S_1$ by $(s,t)^\beta = s^{-1}t$. For any $(s_1,t_1), (s_2,t_2) \in G$ we have

$$\begin{aligned}((s_1,t_1)(s_2,t_2))^\beta &= (s_1 s_2, t_1 t_2)^\beta = (s_1 s_2)^{-1} t_1 t_2 = (s_1^{-1} t_1)^{s_2} (s_2^{-1} t_2) \\ &= ((s_1,t_1)^\beta)^{s_2} (s_2,t_2)^\beta = ((s_1,t_1)^\beta)^{(s_2,t_2)^{\alpha_1}} (s_2,t_2)^\beta,\end{aligned}$$

and hence $\beta \in Z^1_X(G, S_1)$. Moreover for any x in S and $(s,t) \in G$ we have

$$x^{(s,t)^{\alpha_1}(s,t)^{\beta}} = x^{ss^{-1}t} = x^t = x^{(s,t)^{\alpha_2}},$$

so that $S_2 = (S_1)_\beta$ and S_1 and S_2 are (G,X)-equivalent. Clearly S_1 is G-irreducible, while if $T < S$, then T is a proper G-subgroup of S_2.

Another example is the following:

Example 5. Let $G = \mathrm{Alt}(6)$, $N = \mathrm{Alt}(5)^6$ and consider the following elements of G: $t_1 = (1,6), t_2 = (2,6), \ldots, t_5 = (5,6), t_6 = 1$. If $g \in G$ and $i \in \{1, \ldots, 6\}$, then $6(t_{ig^{-1}} g t_i) = 6$, and hence $t_{ig^{-1}} g t_i$ can be viewed as an element of $\mathrm{Alt}(5)$. Define actions $\alpha_i : G \to \mathrm{Aut}\, N$ for $i = 1, 2$ in the following way:

$$(x_1, \ldots, x_6)^{g^{\alpha_1}} = (x_{1g^{-1}}, \ldots, x_{6g^{-1}}),$$
$$(x_1, \ldots, x_6)^{g^{\alpha_2}} = (x_{1g^{-1}}{}^{t_{1g^{-1}} g t_1}, \ldots, x_{6g^{-1}}{}^{t_{6g^{-1}} g t_6}).$$

Denote by N_1 and N_2 the G-groups corresponding to these two actions. Define $\beta : G \to N_1$ by $g^\beta = (t_{1g^{-1}} g t_1, \ldots, t_{6g^{-1}} g t_6)$; since $\beta \in Z^1(G, N_1)$ and $n^{g^{\alpha_2}} = n^{g^{\alpha_1} g^\beta}$ for any $n \in N$, $g \in G$, then N_1 and N_2 are G-equivalent. The semidirect product $N \rtimes_{\alpha_2} G$ is isomorphic to the twisted wreath product $\mathrm{Alt}(5)\, \mathrm{twr}_\alpha \mathrm{Alt}(6)$, where α is the embedding obtained by identifying $\mathrm{Alt}(5)$ with the stabilizer of 6 in $\mathrm{Alt}(6)$; this is a primitive permutation group, and so G is a maximal subgroup of $N \rtimes_{\alpha_2} G$ and the action α_2 is irreducible. On the other hand, the diagonal subgroup $\{(x, \ldots, x) \mid x \in \mathrm{Alt}(5)\} \leqslant N$ is G^{α_1}-invariant.

Let $\mathscr{CF}(G)$ be the set of all chief factors of G. Our target is the study of the (G,X)-equivalence relation between elements of the set $\mathscr{CF}(G)$. First we need a definition. Given a G-group A let

$$I_G(A) = \{g \in G \mid g \text{ induces an inner automorphism of } A\}.$$

An immediate consequence of Proposition 2 is that if $A \sim_{G,X} B$, then $I_G(A) = I_G(B)$. When A is abelian, $I_G(A) = C_G(A)$, whereas in the non-abelian case this is not true and it is possible that $C_G(A) \neq C_G(B)$. (In Example 3, $S_1 \sim_{G,X} S_2$ and $I_G(S_1) = I_G(S_2) = G$ but $S_2 = C_G(S_1) \neq C_G(S_2) = S_1$.) However if A is a non-abelian chief factor of G, then $G/C_G(A)$ is a monolithic primitive group, and its socle $I_G(A)/C_G(A)$ is G-isomorphic to A. So if $A, B \in \mathscr{CF}(G)$ and $A \sim_{G,X} B$, then $I_G(A) = I_G(B) = I$ and $I/C_G(A) \cong I/C_G(B)$. We also observe that if A is a non-abelian chief factor and B is a G-group, then the condition $A \sim_{G,X} B$ does not imply $I_G(A)/C_G(A) \cong I_G(B)/C_G(B)$. In Example 4, S_1 can be identified with a chief factor of $G = S \times T$, $S_2 \sim_{G,X} S_1$, but $I_G(S_1)/C_G(S_1) = G/T \cong S$, whereas $I_G(S_2)/C_G(S_2) = G/S \cong T$.

In order to proceed with our discussion, we need another definition.

Definition 6. Let $H_1/K_1, H_2/K_2 \in \mathscr{CF}(G)$. We say that H_1/K_1 and H_2/K_2 are (G, X)-related if either $H_1/K_1 \cong_G H_2/K_2$ or G has a normal subgroup N such that

(i) G/N is a primitive permutation group which contains distinct minimal normal subgroups M_1/N and M_2/N;

(ii) there exists a subgroup U containing $\langle X, N\rangle$ such that U/N is a complement for both M_1/N and M_2/N in G/N;

(iii) $H_1/K_1 \cong_G M_1/N$, $H_2/K_2 \cong_G M_2/N$.

Now we are ready to prove the following generalization of [8, Proposition 1.4].

Proposition 7. *Let $H_1/K_1, H_2/K_2 \in \mathscr{CF}(G)$. Then H_1/K_1 and H_2/K_2 are (G, X)-equivalent if and only if they are (G, X)-related.*

Proof. Assume that H_1/K_1 and H_2/K_2 are (G, X)-equivalent but not G-isomorphic. Then $I_G(H_1/K_1) = I_G(H_2/K_2) = I$, while $C_1 = C_G(H_1/K_1) \neq C_G(H_2/K_2) = C_2$. Set $C = C_1 \cap C_2$. We have

$$B = C_2/C \cong_G I/C_1 \cong_G H_1/K_1 \quad \text{and} \quad A = C_1/C \cong_G I/C_2 \cong_G H_2/K_2.$$

Hence $A \sim_{G,X} B$ and there exists $\beta \in \mathrm{Z}^1_X(G, B)$ such that $A \cong_G B_\beta$; thus $U = \ker\beta$ is the required subgroup of G.

In order to prove the converse it suffices to show that if N_1 and N_2 are minimal normal subgroups of a primitive permutation group G and U is a common complement for N_1 and N_2 in G containing a subset X of G, then $N_1 \sim_{G,X} N_2$. Consider

$$\phi : N_1 \to N_2 \quad \text{and} \quad \beta : G \to N_2$$

given, respectively, by $n_1^\phi = n_2$ if $n_1 n_2 \in U$ and $g^\beta = n_2$ if $g \in G$, $n_2 \in N_2$ and $gn_2 \in U$. Then $\beta \in \mathrm{Z}^1_X(G, N_2)$ and ϕ is a G-isomorphism between N_1 and $(N_2)_\beta$.

Definition 8 (see [4]). Let L be a monolithic primitive group and let A be its unique minimal normal subgroup. For each positive integer k, let L^k be the k-fold product of L. The *crown-based power* of L of size k is the subgroup L_k of L^k defined by

$$L_k = \{(l_1, \ldots, l_k) \in L^k \mid l_1 \equiv \cdots \equiv l_k \bmod A\}.$$

Clearly $\mathrm{soc}(L_k) = A^k$, $L_k/\mathrm{soc}(L_k) \cong L/A$ and the quotient group of L_k over any minimal normal subgroup is isomorphic to L_{k-1}, for $k > 1$. Moreover any normal subgroup of L_k either contains or is contained in $\mathrm{soc}(L_k)$. Furthermore let Q be a subset of L and consider

$$\Delta(Q) = \{(q, \ldots, q) \mid q \in Q\} \leqslant \Delta(L) = \{(l, \ldots, l) \mid l \in L\} \leqslant L_k.$$

Proposition 7 implies that the minimal normal subgroups of L_k are all $(L_k, \Delta(Q))$-equivalent. Indeed, if A is abelian, then they are L_k-isomorphic. Suppose that A is

non-abelian; then the minimal normal subgroups of L_k are precisely the direct factors $A_1, \dots, A_k$ of $\mathrm{soc}(L_k) = A^k$. For $i \neq j$ set $N = \prod_{r \neq i,j} A_r$. Then $A_i \cong_G A_i N/N$ and $A_j \cong_G A_j N/N$; moreover $\Delta(L)N/N$ is a complement for both $A_i N/N$ and $A_j N/N$ in L_k/N, so that A_i and A_j are $(L_k, \Delta(Q))$-related.

We say that a factor H/K of G is X-complemented in G if there exists a subgroup U of G containing X such that $UH = G$ and $U \cap H = K$. An abelian chief factor H/K of G is X-complemented if and only if there exists a maximal subgroup of G which contains $\langle X, K \rangle$ but not H. This does not hold if H/K is non-abelian; nevertheless we have the following criterion, which can be proved arguing as in [8, Proposition 1.3].

Proposition 9. *Let H/K be a non-abelian chief factor of G. Then H/K is X-complemented in G if and only if there exists a G-group B which is (G, X)-equivalent to H/K and satisfies the condition $H \leqslant C_G(B)$.*

We say that a chief factor H/K of G is X-Frattini if it is abelian and not X-complemented. If $X = \varnothing$, or more in general if $X \subseteq \mathrm{Frat}\, G$, then H/K is X-Frattini if and only if $H/K \leqslant \mathrm{Frat}(G/K)$.

Definition 10. Let A be an irreducible G-group, and consider the set $\mathscr{N}_{G,X}(A)$ of normal subgroups N of G which satisfy the following properties:

(i) $N \leqslant I_G(A)$;

(ii) $I_G(A)/N \sim_{G,X} A$;

(iii) $I_G(A)/N$ is not an X-Frattini chief factor.

We define $R_{G,X}(A) = \bigcap_{N \in \mathscr{N}_{G,X}(A)} N$, if $\mathscr{N}_{G,X}(A) \neq \varnothing$ and $R_{G,X}(A) = I_G(A)$ otherwise.

We set $R_{G,\varnothing}(A) = R_G(A)$; clearly $R_G(A) \leqslant R_{G,X}(A) \leqslant I_G(A)$. The quotient group $I_G(A)/R_G(A)$ is called the A-crown of G, as described in [5], [8]; generalizing this definition we call $I_G(A)/R_{G,X}(A)$ the (G, X)-crown associated with A. Note that two (G, X)-equivalent G-groups define the same (G, X)-crown.

We want to study the structure of $G/R_{G,X}(A)$ when $R_{G,X}(A) \neq I_G(A)$, i.e. when A is (G, X)-equivalent to a non-X-Frattini chief factor of G; in the sequel we shall assume A to be a chief factor of G.

Let $\rho : G \to \mathrm{Aut}\, A$ such that $g^\rho : a \mapsto a^g$ for all $a \in A$. The *monolithic primitive group associated with A* is defined as

$$L_G(A) = \begin{cases} G^\rho A \cong A \rtimes (G/C_G(A)) & \text{if } A \text{ is abelian,} \\ G^\rho \cong G/C_G(A) & \text{otherwise.} \end{cases}$$

We define

$$Q_{G,X}(A) = X^\rho.$$

When A is abelian, $A = \mathrm{soc}(L_G(A))$ is $Q_{G,X}(A)$-complemented in $L_G(A)$.

If a chief factor B is (G,X)-equivalent to A, then there exists an isomorphism $\gamma : L_G(A) \to L_G(B)$ such that $(Q_{G,X}(A))^\gamma = Q_{G,X}(B)$. This follows immediately from the definition when A and B are abelian, since then $C_G(A) = C_G(B)$. Therefore assume that A is non-abelian. Then $A \sim_{G,X} B$ and $B \cong_G I_G(B)/C_G(B)$, so that there exists $\beta \in Z^1_X(G, I_G(B)/C_G(B))$ such that $A \cong_G (I_G(B)/C_G(B))_\beta$. Now we define $\gamma : L_G(A) \cong G/C_G(A) \to L_G(B) \cong G/C_G(B)$ by $(gC_G(A))^\gamma = gg^\beta C_G(B)$.

The existence of an isomorphism $\gamma : L_G(A) \to L_G(B)$ such that

$$(Q_{G,X}(A))^\gamma = Q_{G,X}(B)$$

does not imply that $A \sim_{G,X} B$. For example let S be a non-abelian simple group and let Y be a subset of S containing at least one element $s \neq 1$. Take $G = S^2$ and $X = Y^2 \subseteq G$. If S_1 and S_2 are the two direct factors of G, then the map $\gamma : G/C_G(S_1) \to G/C_G(S_2)$ defined by $((s_1,s_2)C_G(S_1))^\gamma = (s_1,s_2)C_G(S_2)$ is an isomorphism between $L_G(S_1)$ and $L_G(S_2)$ such that $(Q_{G,X}(A))^\gamma = Q_{G,X}(B)$. However S_1 and S_2 have no common complement in G containing X, and so, by Proposition 7, S_1 and S_2 are not (G,X)-equivalent.

Let A be a chief factor of G. To simplify our notation we identify A with $\mathrm{soc}(L_G(A))$ and we set $I = I_G(A)$, $R = R_G(A)$, $R_X = R_{G,X}(A)$, $L = L_G(A)$, $Q = Q_{G,X}(A)$ and $\mathcal{N} = \mathcal{N}_{G,X}(A)$.

Lemma 11. *If $N \in \mathcal{N}$, then there exists an epimorphism: $\eta : G \to L$ such that*

(1) $\ker\eta = N$;

(2) $I^\eta = A$;

(3) $g^\eta \equiv g^\rho \bmod A$ *for each* $g \in G$;

(4) $x^\eta = x^\rho$ *for each* $x \in X$;

(5) *if A is abelian, then G^ρ is a complement for A in L and it contains $Q = X^\rho$.*

Proof. There exist $\beta \in Z^1_X(G,A)$ and an isomorphism $\phi : I/N \to A$ such that $a^{\phi^{-1}g\phi} = a^{gg^\beta}$, for all $a \in A$ and $g \in G$. If A is abelian, then $I = C_G(A)$ and, as I/N is X-complemented in G, there exists a subgroup U of G such that $X \subseteq U$, $IU = G$ and $I \cap U = N$. We define $\eta : G \to A \rtimes \mathrm{Aut}\, A$ by setting $g^\eta = (cN)^\phi u^\rho$ where $g = cu$ with $u \in U$ and $c \in I$. If A is non-abelian, then define $\eta : G \to \mathrm{Aut}\, A$ by $a^{g^\eta} = a^{\phi^{-1}g\phi}$. We have $g^\eta = g^\rho y$ where y is the inner automorphism of A induced by conjugation with g^β; in particular $y \in \mathrm{soc}\, L$. Let $g \in \ker\beta$. If A is abelian then $g^\eta = (cN)^\phi u^\rho = 1$ implies that $g \in I \cap U = N$. If A is non-abelian then $g^\eta = 1$ if and only if $g \in C_G(I/N) = N$. In both cases, $\ker\eta = N$ and $G^\eta = L$. Finally let $x \in X$. If A is non-abelian, then $x^\eta = x^\rho$ since $x^\beta = 1$; if A is abelian, then $x \in U$ and again $x^\eta = x^\rho$.

The next result explains the role played by the crown-based powers in the study of G/R_X.

Proposition 12. *There exist $\delta = \delta_{G,X}(A) \in \mathbb{N}$ and an epimorphism $\alpha : G \to L_\delta$ such that*

(1) $\ker \alpha = R_X$;

(2) $X^\alpha = \Delta(Q) = \{(q, \dots, q) \mid q \in Q\} \leqslant \Delta(L) = \{(l, \dots, l) \mid l \in L\}$;

(3) $\mathrm{soc}(L_\delta)$ *is X^α-complemented if A is abelian.*

Proof. Let $\rho : G \to \mathrm{Aut}\, A$ be the homomorphism induced by the conjugation action of G on A. Assume that $\{U_1, \dots, U_\delta\}$ is a minimal subset of $\mathscr{N}$ such that $\bigcap_{1 \leqslant i \leqslant \delta} U_i = R_X$. For each $i \in \{1, \dots, \delta\}$ let $\eta_i : I/U_i \to L$ be the epimorphism defined in Lemma 11. Note that $g^{\eta_i} \equiv g^{\eta_j} \bmod A$, and so we may define a homomorphism $\alpha : G \to L_\delta$ by setting $g^\alpha = (g^{\eta_1}, \dots, g^{\eta_\delta})$. We have $\ker \alpha = \bigcap_i \ker \eta_i = \bigcap_i U_i = R_X$. For $i \in \{1, \dots, \delta\}$ let $N_i = \bigcap_{j \neq i} U_j$. It can easily be seen that $N_i^{\eta_i} = A$ while $N_i^{\eta_j} = 1$ if $i \neq j$; thus α is surjective. If $x \in X$ then $x^\alpha = (x^\rho, \dots, x^\rho) \in \Delta(Q)$. When A is abelian, we deduce from Lemma 11 that $\Delta(G^\rho)$ is a complement of $\mathrm{soc}(L_\delta) = A^\delta$ in L_δ and contains X^α.

This proposition has the following consequence:

Lemma 13. *Let H/K be a chief factor of G. If $R_X \leqslant K < H \leqslant I$, then H/K is (G, X)-equivalent to A and is non-X-Frattini.*

Proof. Let $\mathscr{C}$ be the set of chief factors H/K such that $R_X \leqslant H \leqslant K \leqslant I$ and let $\alpha : G \to L_\delta$ be the epimorphism defined in Proposition 12. It can easily be seen that if $H_1/K_1, H_2/K_2 \in \mathscr{C}$, then the chief factors H_1^α/K_1^α and H_2^α/K_2^α are (L_δ, X^α)-related; this implies that H_1/K_1 and H_2/K_2 are (G, X)-related. Hence all factors in $\mathscr{C}$ are (G, X)-equivalent, and in particular they are (G, X)-equivalent to A, as $I/N \in \mathscr{C}$ for any $N \in \mathscr{N}$. Moreover, if A is abelian, then H^α/K^α is X^α-complemented in L_δ, and hence H/K is X-complemented in G. We conclude that H/K is non-X-Frattini.

We can also prove a converse result:

Lemma 14. *Let H/K be a chief factor of G. Then H/K is non-X-Frattini and (G, X)-equivalent to A if and only if $R_X H/R_X K \neq 1$ and $R_X H \leqslant I$.*

Proof. If $R_X K \neq R_X H \leqslant I$, then, by Lemma 13, $R_X H/R_X K$ is non-X-Frattini and (G, X)-equivalent to A; hence also H/K satisfies these properties.

Now assume that the chief factor H/K is non-X-Frattini and is (G, X)-equivalent to A. There exists a maximal subgroup, say M, which contains K but not H. Let N be the normal core of M in G. Since H and K are normal in G, from $K \leqslant M$ and $H \not\leqslant M$ we deduce that $K \leqslant N$ and $H \not\leqslant N$. In particular HN/N is a minimal normal subgroup of the primitive group G/N and it is G-isomorphic to H/K, hence (G, X)-equivalent to A; moreover when H/K is abelian, since H/K is X-complemented in G, we may assume that $X \subseteq M$, so that HN/N is X-complemented. By the definition of $I = I_G(A)$, the socle of the primitive group G/N is I/N. Then either $I/N = HN/N$

and $N \in \mathscr{N}_X$ or G/N is a primitive group with distinct non-abelian minimal normal subgroups HN/N and Y/N. In the first case $R_X \leqslant N = NK < NH = I$ and thus $R_X K \neq R_X H \leqslant I$. In the second case $I/N = HN/N \times Y/N$, so that $I/Y \cong_G HN/N$ is non-abelian and (G, X)-equivalent to A; this implies that $Y \in \mathscr{N}_X$ and $R_X \leqslant Y$. We deduce that $R_X H \leqslant YH \leqslant I$; moreover $R_X K \leqslant R_X N \leqslant Y$, while $H \not\leqslant Y$, and hence $R_X K < R_X H$.

Theorem 15. *Each chief series of G contains exactly $\delta_{G,X}(A)$ factors which are non-X-Frattini and are (G, X)-equivalent to A.*

Proof. Let $\Sigma : 1 = G_t < G_{t-1} < \cdots < G_0 = G$ be a chief series of G. For $0 \leqslant i \leqslant t$ define $H_i = G_i R_X$. If $i < t$ then either $H_i = H_{i+1}$ or H_i/H_{i+1} is a chief factor of G/R_X. Moreover the set of non-trivial factors H_i/H_{i+1} coincides with the set of factors of a chief series of G/R_X. Since a normal subgroup N/R_X of G/R_X either contains I/R_X or is contained in I/R_X, either $H_i \leqslant I$ or $H_i \geqslant I$. Let j be the smallest integer such that $H_j \leqslant I$. Lemma 14 implies that if $i < j$ then G_i/G_{i+1} cannot be non-X-Frattini and (G, X)-equivalent to A. Moreover, if $i \geqslant j$, then $H_i/H_{i+1} \neq 1$ if and only if G_i/G_{i+1} is non-X-Frattini and (G, X)-equivalent to A. Let $\Theta = \{G_{i_1}/G_{i_1+1}, \ldots, G_{i_\delta}/G_{i_\delta+1}\}$ be the set of factors of Σ which are non-X-Frattini and (G, X)-equivalent to A and assume that $i_1 < i_2 < \cdots < i_\delta$. From above we have

$$I = H_{i_1} > H_{i_1+1} = H_{i_2} > \cdots > H_{i_j+1} = H_{i_{j+1}} > \cdots > H_{i_{\delta+1}} = R$$

and $H_{i_j}/H_{i_{j+1}}$ is a chief factor of G; in particular $\delta = |\Theta|$ does not depend on Σ and it coincides with $\delta_{G,X}(A)$.

3 The Dirichlet polynomial $P_G(X, s)$

We define a Dirichlet polynomial $P_G(X, s)$ as follows:

$$P_G(X, s) := \sum_{n \in \mathbb{N}} \frac{a_n}{n^s} \quad \text{with } a_n := \sum_{\substack{|G:H|=n, \\ X \subseteq H \leqslant G}} \mu(H, G),$$

where μ is the Möbius function of the subgroup lattice of G. When t is a positive integer, $P_G(X, t)$ is the probability that t random elements generate G together with the elements of X. The ring $\mathscr{D}$ of Dirichlet polynomials is a unique factorization domain. If $N \trianglelefteq G$, then we may consider the Dirichlet polynomial $P_{G/N}(XN, s)$, where $XN = \{xN \mid x \in X\}$; this polynomial divides $P_G(X, s)$ in the ring $\mathscr{D}$. More precisely, we have the following result.

Proposition 16. *If N is a normal subgroup of a finite group G, then*

$$P_G(X, s) = P_{G/N}(XN, s) P_{G,N}(X, s)$$

where

$$P_{G,N}(X,s) := \sum_{n\in\mathbb{N}} \frac{b_n}{n^s} \quad \textit{with } b_n := \sum_{\substack{|G:H|=n \\ X\subseteq H\leqslant G \\ HN=G}} \mu(H,G).$$

This proposition will be proved by applying the complement theorem of Crapo:

Theorem 17 ([3], Theorem 12). *Let $\mathscr{L}$ be a finite lattice and fix $x\in\mathscr{L}$. Let $x^\perp = \{y\in\mathscr{L} \mid x\wedge y = 0, x\vee y = 1\}$. Then*

$$\mu_{\mathscr{L}}(0,1) = \sum_{\substack{y,z\in x^\perp \\ y\leqslant z}} \mu_{\mathscr{L}}(0,y)\mu_{\mathscr{L}}(z,1).$$

In particular, if $x^\perp$ is an antichain, then

$$\mu_{\mathscr{L}}(0,1) = \sum_{y\in x^\perp} \mu_{\mathscr{L}}(0,y)\mu_{\mathscr{L}}(y,1).$$

Proof of Proposition 16. Let H be a subgroup of G. We apply Theorem 17 to the lattice $\mathscr{L}_H$ of subgroups of G containing H and we take $x = HN$. Let us define

$$\mathscr{S}_H := \{Y\leqslant G \mid H\leqslant Y, YN = G, Y\cap N = H\cap N\};$$

we have $x^\perp = \{Y\leqslant G \mid H\leqslant Y, \langle Y, HN\rangle = G, Y\cap HN = H\} = \mathscr{S}_H$. Notice that if $Y\in\mathscr{S}_H$ then $|G:Y| = |N:N\cap H|$, and hence $x^\perp$ is an antichain and by Theorem 17

$$\mu(H,G) = \sum_{Y\in\mathscr{S}_H} \mu(H,Y)\mu(Y,G).$$

Consequently

$$\begin{aligned} P_G(X,s) &= \sum_{X\subseteq H\leqslant G} \frac{\mu(H,G)}{|G:H|^s} = \sum_{X\subseteq H\leqslant G} \left(\sum_{Y\in\mathscr{S}_H} \frac{\mu(H,Y)}{|Y:H|^s} \frac{\mu(Y,G)}{|G:Y|^s} \right) \\ &= \sum_{\substack{X\subseteq Y\leqslant G \\ YN=G}} \left(\frac{\mu(Y,G)}{|G:Y|^s} \left(\sum_{H\in\mathscr{T}_Y} \frac{\mu(H,Y)}{|Y:H|^s} \right) \right) \end{aligned}$$

with $\mathscr{T}_Y = \{H \mid X\subseteq H\leqslant Y, H\cap N = Y\cap N\}$. Now fix Y with the properties $X\subseteq Y$ and $YN = G$ and let $\mathscr{L}_{XN}$ be the lattice of subgroups of G containing $\langle X, N\rangle$. It can

easily be verified that $H \mapsto HN$ induces an isomorphism between $\mathscr{T}_Y$ and $\mathscr{L}_{XN}$ (with inverse the map $K \mapsto K \cap Y$); this implies that

$$\mu_{\mathscr{T}_Y}(H, Y) = \mu_{\mathscr{L}_{XN}}(HN, YN) = \mu_{\mathscr{L}_{XN}}(HN, G) = \mu(HN, G).$$

Moreover if $H \in T_Y$ and $H \leqslant K \leqslant Y$, then $K \in T_Y$ and so

$$\mu(H, Y) = \mu_{\mathscr{T}_Y}(H, Y) = \mu(HN, G).$$

In addition, if $H \in \mathscr{T}_Y$, then $|Y : H| = |G : HN|$. This implies that

$$\begin{aligned}
P_G(X, s) &= \sum_{\substack{X \subseteq Y \leqslant G \\ YN = G}} \left(\frac{\mu(Y, G)}{|G : Y|^s} \left(\sum_{H \in \mathscr{T}_Y} \frac{\mu(H, Y)}{|Y : H|^s} \right) \right) \\
&= \sum_{\substack{X \subseteq Y \leqslant G \\ YN = G}} \left(\frac{\mu(Y, G)}{|G : Y|^s} \left(\sum_{K \in \mathscr{L}_{XN}} \frac{\mu(K, G)}{|G : K|^s} \right) \right) \\
&= \sum_{\substack{X \subseteq Y \leqslant G \\ YN = G}} \left(\frac{\mu(Y, G)}{|G : Y|^s} P_{G/N}(XN, s) \right) \\
&= P_{G/N}(XN, s) \sum_{\substack{X \subseteq Y \leqslant G \\ YN = G}} \frac{\mu(Y, G)}{|G : Y|^s} \\
&= P_{G/N}(XN, s) P_{G,N}(X, s),
\end{aligned}$$

and so we have proved our statement.

Notice that if a chief factor H/K of G is X-Frattini, then $P_{G/K, H/K}(XK, s) = 1$. Hence, by taking a chief series

$$\Sigma : 1 = N_l < \cdots < N_1 < N_0 = G$$

and iterating Proposition 16, we obtain an expression of $P_G(X, s)$ as a product indexed by the non-X-Frattini chief factors in the series

$$P_G(X, s) = \prod_{\substack{N_i/N_{i+1} \\ \text{non-}X\text{-Frattini}}} P_{G/N_{i+1}, N_i/N_{i+1}}(XN_{i+1}, s). \tag{3.1}$$

Now our aim is to describe the factors in (3.1). In order to do this we need a definition.

Let L be a finite monolithic primitive group, and let A be its socle. Assume also that $Q \subseteq L$ and that A is Q-complemented when A is abelian. We define

$$\begin{aligned}\tilde{P}_{L,1}(Q,s) &= P_{L,A}(Q,s),\\ \tilde{P}_{L,i}(Q,s) &= P_{L,A}(Q,s) - \frac{(1+q+\cdots+q^{i-2})\gamma}{|A|^s},\end{aligned} \tag{3.2}$$

where $\gamma = |C_{\mathrm{Aut}\,L}(L/A) \cap C_{\mathrm{Aut}\,L}(Q)|$ and $q = |\mathrm{End}_L A|$ if A is abelian and $q = 1$ otherwise.

Lemma 18. *Let L be a finite monolithic primitive group, with socle A. Let $G = L_\delta$ for a positive integer δ, and assume that N is a minimal normal subgroup of G. Suppose that $Q \subseteq L$ and that A is Q-complemented when A is abelian. Then*

$$P_{G,N}(\Delta(Q),s) = \tilde{P}_{L,\delta}(Q,s).$$

Proof. For $\delta = 1$ there is nothing to prove. Assume that $\delta > 1$. We have $\mathrm{soc}(G) = A_1 \times \cdots \times A_\delta$ and we may identify N with A_δ. Write $M = A_1 \times \cdots \times A_{\delta-1}$. Define

$$\mathscr{S} = \{H \leqslant G \mid \Delta(Q) \leqslant H, HN = G\}, \quad \mathscr{S}_1 = \{H \in \mathscr{S} \mid M \leqslant H\}, \quad \text{and} \quad \mathscr{S}_2 = \mathscr{S} \setminus \mathscr{S}_1.$$

By Proposition 16, $P_{G,N}(\Delta(Q),s) = P_1(s) + P_2(s)$, with

$$P_1(s) = \sum_{H \in \mathscr{S}_1} \frac{\mu(H,G)}{|G:H|^s}, \quad P_2(s) = \sum_{H \in \mathscr{S}_2} \frac{\mu(H,G)}{|G:H|^s}.$$

Let $\pi : G \to L$ be the restriction to $G = L_\delta \leqslant L^\delta$ of the projection $\pi_\delta : L^\delta \to L$ onto the δth factor and let $\mathscr{T} = \{T \leqslant L \mid Q \leqslant T, TA = L\}$. The map $H \to H^\pi$ defines a bijection between $\mathscr{S}_1$ and $\mathscr{T}$; moreover $\mu(H,G) = \mu(H^\pi, L)$ and $|G:H| = |L:H^\pi|$, so that

$$P_1(s) = \sum_{H \in \mathscr{S}_1} \frac{\mu(H,G)}{|G:H|^s} = \sum_{H \in \mathscr{S}_1} \frac{\mu(H^\pi,L)}{|L:H^\pi|^s} = \sum_{T \in \mathscr{T}} \frac{\mu(T,L)}{|L:T|^s} = P_{L,A}(Q,s).$$

Now assume that $H \in \mathscr{S}_2$ and let $K = H \cap M$. Then K is a normal subgroup of $G = HN$ as $[M,N] = 1$, and hence $K \cong A^i$ with $i \leqslant \delta - 2$. Since $HN = G$ we have

$$|G:H| = |N : H \cap N| \leqslant |N| = |A|, \tag{3.3}$$

while

$$|G:H| \geqslant |MH:H| = |M : H \cap M| = |M:K| = |A|^{\delta-1-i}. \tag{3.4}$$

Comparing (3.3) and (3.4) we deduce that H has the following properties:

(1) $K = M \cap H$ is the direct product of $\delta - 2$ minimal normal subgroups of G;

(2) $G/K \cong L_2$, and H/K is a common complement of the minimal normal subgroups NK/K and M/K of $G/K \cong L_2$ and it contains $\Delta(Q)K/K$.

Conversely, if H is a subgroup which contains a normal subgroup K of G in such a way that the previous properties are satisfied, then $H \in \mathscr{S}_2$.

Note that the subgroups of L_2 which are complements of two distinct minimal normal subgroups and contain $\{(q,q) \mid q \in Q\}$ are precisely those of the form $\{(l, l^\alpha) \mid l \in L\}$, with $\alpha \in C_{\mathrm{Aut}\,L}(L/A) \cap C_{\mathrm{Aut}\,L}(Q)$. Thus a subgroup H with the previous properties is uniquely determined by K and α. The number of choices for K is $1 + q + \cdots + q^{\delta-2}$, while the number of choices for α is γ. Moreover a subgroup H which satisfies (1) and (2) is a maximal subgroup of G, and so $\mu(H, G) = -1$ for each $H \in \mathscr{S}_2$. Hence

$$P_2(s) = \sum_{H \in \mathscr{S}_2} \frac{\mu(H,G)}{|G:H|^s} = \sum_{H \in \mathscr{S}_2} \frac{-1}{|A|^s} = -\frac{(1 + q + \cdots + q^{\delta-2})\gamma}{|A|^s}$$

and the proof is complete.

Theorem 19. *Let $A = H/K$ be a non-X-Frattini chief factor of G. If $R_X = R_{G,X}(A)$ then*

$$P_{G/K,H/K}(XK, s) = P_{G/R_XK,\, R_XH/R_XK}(XR_XK, s) = \tilde{P}_{L,k}(Q, s),$$

where $L = L_G(A)$, $Q = Q_{G,X}(A)$ and $k = \delta_{G/K,XK}(A)$.

Proof. Let $\mathscr{S} = \{U \leqslant G \mid X \subseteq U, K \leqslant U, UH = G, \text{ and } \mu(U,G) \neq 0\}$; notice that

$$P_{G/K,H/K}(XK, s) = \sum_{U \in \mathscr{S}} \frac{\mu(U,G)}{|G:U|^s}.$$

Observe that $\mu(U,G) \neq 0$ only if U is intersection of maximal subgroups of G. Now let M be a maximal subgroup of G containing U and let N be the normal core of M in G; HN/N is a minimal normal subgroup of the primitive group G/N and it is G-isomorphic to H/K, and hence (G,X)-equivalent to A; when H/K is abelian, HN/N is also X-complemented. By the definition of $I = I_G(A)$, the socle of the primitive group G/N is I/N. Then either $I/N = HN/N$ and $N \in \mathscr{N}_{G,X}(A)$ or G/N is a primitive group with two distinct non-abelian minimal normal subgroups HN/N and Y/N. In the second case $I/N = HN/N \times Y/N$ and M/N is a common complement for HN/N and Y/N in G/N, so that $HN/N \sim_{G,X} Y/N \sim_{G,X} A$; since $I/HN \cong_G Y/N$ and $I/Y \cong_G HN/N$, both HN and Y belong to $\mathscr{N}_{G,X}(A)$. In each case we deduce that $R_X \leqslant N \leqslant M$. Hence $R_XK \leqslant U$ for any $U \in \mathscr{S}$. This implies immediately that $P_{G/K,H/K}(XK, s) = P_{G/R_XK,\, R_XH/R_XK}(XR_XK, s)$. Combining Proposition 12 and Lemma 18, we conclude that $P_{G/R_XK,\, R_XH/R_XK}(XR_XK, s) = \tilde{P}_{L,k}(Q, s)$.

Since in any chief series of G the number of non-X-Frattini factors (G,X)-equivalent to A is precisely $\delta_{G,X}(A)$, we get that the total contribution to $P_G(X,s)$ from these factors is $\prod_{1\leqslant i\leqslant \delta_{G,X}(A)} \tilde{P}_{L_G(A),i}(Q_{G,X}(A),s)$. Thus, given a chief series $1=N_l<\cdots<N_0=G$, we can collect together the (G,X)-equivalent terms and we obtain

$$\begin{aligned} P_G(X,s) &= \prod_{\substack{N_i/N_{i+1}\\ \text{non-}X\text{-Frattini}}} P_{G/N_{i+1},N_i/N_{i+1}}(XN_{i+1},s)\\ &= \prod_A \left(\prod_{N_i/N_{i-1}\sim_{G,X}A} P_{G/N_{i+1},N_i/N_{i+1}}(XN_{i+1},s)\right)\\ &= \prod_A \left(\prod_{1\leqslant i\leqslant \delta_{G,X}(A)} \tilde{P}_{L_G(A),i}(Q_{G,X}(A),s)\right) \end{aligned}$$

where A runs over a set of representatives of the (G,X)-equivalence classes of non-X-Frattini chief factors of G. Thus we get the following factorization, which is independent of the choice of the chief series.

Theorem 20. *Let G be a finite group. Then*

$$P_G(X,s)=\prod_A \left(\prod_{1\leqslant i\leqslant \delta_{G,X}(A)} \tilde{P}_{L_G(A),i}(Q_{G,X}(A),s)\right) \tag{3.5}$$

where A runs over a set of representatives of the (G,X)-equivalence classes of non-X-Frattini chief factors of G. Moreover, the factorization of $P_G(X,s)$ corresponding to the non-X-Frattini factors in a chief series Σ of G is precisely (3.5)*, independently of the choice of Σ.*

Corollary 21. *Let $t\in\mathbb{N}$. Then there exist $g_1,\dots,g_t$ such that $G=\langle X,g_1,\dots,g_t\rangle$ if and only if $\tilde{P}_{L_G(A),\delta_{G,X}(A)}(Q_{G,X}(A),t)>0$ for any non-X-Frattini chief factor A of G.*

Proof. Recall that $P_G(X,t)$ is the probability that t random elements together with the elements of X generate G. Thus there exist $g_1,\dots,g_t$ such that $G=\langle X,g_1,\dots,g_t\rangle$ if and only if $P_G(X,t)>0$. By definition, if $i\leqslant\delta_{G,X}(A)$ then

$$\tilde{P}_{L_G(A),i}(Q_{G,X}(A),t)\geqslant \tilde{P}_{L_G(A),\delta_{G,X}(A)}(Q_{G,X}(A),t),$$

and so if $\tilde{P}_{L_G(A),\delta_{G,X}(A)}(Q_{G,X}(A),t)>0$ for any non-X-Frattini chief factor A of G then

$$P_G(X,t)=\prod_A \left(\prod_{1\leqslant i\leqslant \delta_{G,X}(A)} \tilde{P}_{L_G(A),i}(Q_{G,X}(A),t)\right)>0.$$

Conversely, assume that $P_G(X,t) > 0$ and let A be a non-X-Frattini chief factor of G. We want to prove that $\tilde{P}_{L,\delta}(Q,t) > 0$, where $L = L_G(A)$, $\delta = \delta_{G,X}(A)$ and $Q = Q_{G,X}(A)$. Let $R = R_{G,X}(A)$ and let N/R be a minimal normal subgroup of G/R. By Theorem 19,

$$\tilde{P}_{L,\delta}(Q,t) = P_{G/R,N/R}(XR,t) = \frac{P_{G/R}(XR,t)}{P_{G/N}(XN,t)};$$

clearly $P_{G/N}(XN,t) > P_{G/R}(XR,t) > P_G(X,t) > 0$, and so we reach our conclusion.

Suppose that H is a finite group and let A be an abelian irreducible H-group. It is well known (see for example [1]) that

$$|\mathrm{Z}^1(H,A)| = q^{\delta}|\mathrm{Z}^1(H/C_H(A),A)| \tag{3.6}$$

where $q = |\mathrm{End}_H A|$ and $\delta = \delta_{H,\varnothing}(A)$ is the number of non-Frattini factors H-isomorphic to A in a chief series of H. This result can be generalized as follows:

Proposition 22. *Suppose that H is a finite group and let A be an abelian irreducible H-group. If $X \subseteq H$, then*

$$|\mathrm{Z}^1_X(H,A)| = q^{\delta_{H,X}(A)}|\mathrm{Z}^1_{Q_{H,X}(A)}(H/C_H(A),A)|.$$

Proof. Let $G = HA$; note that $P_{G,A}(X,s) = 1 - c/|A|^s$ where c is the number of complements of A in G containing X. These complements are precisely the subgroups of G of the form $H_\beta = \{hh^\beta \mid h \in H\}$, with $\beta \in \mathrm{Z}^1_X(H,A)$. Hence

$$P_{G,A}(X,s) = 1 - \frac{|\mathrm{Z}^1_X(H,A)|}{|A|^s}. \tag{3.7}$$

Let $L = L_G(A)$, $Q = Q_{G,X}(A)$, $\gamma = |C_{\mathrm{Aut}\,L}(L/A) \cap C_{\mathrm{Aut}\,L}(Q)|$ and

$$q = |\mathrm{End}_L A| = |\mathrm{End}_H A|.$$

It can easily be verified that

$$\gamma = (q-1)|\mathrm{Z}^1_Q(L/A,A)|. \tag{3.8}$$

Moreover $H/C_H(A) \cong L/A$ and

$$P_{L,A}(Q,s) = 1 - \frac{|\mathrm{Z}^1_Q(L/A,A)|}{|A|^s}. \tag{3.9}$$

Let $\delta = \delta_{H,X}(A)$. Since $\delta_{G,X}(A) = \delta + 1$, by Theorem 19 we have

$$1-\frac{|Z_X^1(H,A)|}{|A|^s}=P_{G,A}(X,s)=\tilde{P}_{L,\delta+1}(Q,s)$$
$$=1-\frac{|Z_Q^1(L/A,A)|}{|A|^s}-\frac{(1+q+\cdots+q^{\delta-1})\gamma}{|A|^s}$$
$$=1-\frac{|Z_Q^1(L/A,A)|}{|A|^s}-\frac{(1+q+\cdots+q^{\delta-1})(q-1)|Z_Q^1(L/A,A)|}{|A|^s}$$
$$=1-\frac{q^\delta|Z_Q^1(L/A,A)|}{|A|^s}$$

and hence $|Z_X^1(H,A)|=q^\delta|Z_Q^1(L/A,A)|$.

4 An application

Denote by $d(G)$ the smallest cardinality of a set of generators of G. Given an element $g\in G$ we ask whether there exists a set of cardinality $d(G)$ which contains g and generates G. This is equivalent to asking whether

$$P_G(\{g\},d(G)-1)>0. \tag{4.1}$$

Let $X=\{g\}$. By Corollary 21, the condition (4.1) is satisfied if and only if for any non-X-Frattini chief factor A of G the following holds:

$$\tilde{P}_{L_G(A),\delta_{G,X}(A)}(Q_{G,X}(A),d(G)-1)>0. \tag{4.2}$$

Let

$$\Omega_G=\{A\mid \tilde{P}_{L_G(A),\delta_G(A)}(\varnothing,d(G)-1)\leqslant 0\}.$$

If $A\notin\Omega_G$, then $\tilde{P}_{L_G(A),\delta_{G,X}(A)}(Q_{G,X}(A),d(G)-1)\geqslant\tilde{P}_{L_G(A),\delta_G(A)}(\varnothing,d(G)-1)>0$, and so it suffices to verify condition (4.2) just for $A\in\Omega_G$. On the other hand if $A\in\Omega_G$ and $g\in R_G(A)$, then $R_{G,X}(A)=R_G(A)$, $\delta_{G,X}(A)=\delta_G(A)$, $Q_{G,X}(A)=1$ and (4.2) does not hold; therefore $P_G(\{g\},d(G)-1)>0$ implies that $g\notin\bigcup_{A\in\Omega_G}R_G(A)$. This last condition is also sufficient when G is supersoluble.

Theorem 23. *Let G be a supersoluble group and fix $g\in G$. There exists a subset of G of cardinality $d(G)$ which contains g and generates G if and only if $g\notin\bigcup_{A\in\Omega_G}R_G(A)$.*

Proof. Let $A\in\Omega_G$; to prove our theorem it suffices to show that if $g\notin R_G(A)$ then (4.2) holds. We may assume that $R_G(A)=1$, so that $G\cong L_\delta$ with $L=L_G(A)$ and $\delta=\delta_G(A)$. Since A is isomorphic to a chief factor of G and G is supersoluble, $|A|=|\mathrm{End}_L A|=q$ is a prime number. Let N be a minimal normal subgroup of G; arguing as in the proof of Proposition 22 we deduce that

$$\tilde{P}_{L,\delta}(\varnothing, s) = P_{G,N}(\varnothing, s) = 1 - \frac{q^{\delta-1}|\mathrm{Z}^1(L/A, A)|}{q^s}.$$

Moreover $\mathrm{Z}^1(L/A, A) = \{\beta_a \mid a \in A\}$ where $(Al)^{\beta_a} = [a, l]$, and hence

$$|\mathrm{Z}^1(L/A, A)| = q^{\theta},$$

where $\theta = 1$ if $A \neq L$ and $\theta = 0$ otherwise. Consequently $\tilde{P}_{L,\delta}(\varnothing, s) = 1 - q^{\delta-1+\theta-s}$. Since $A \in \Omega_G$, we have $\tilde{P}_{L,\delta}(\varnothing, d(G) - 1) \leqslant 0$ so that $d(G) \leqslant \delta + \theta$. On the other hand, since $P_G(d(G)) > 0$ we have $d(G) > \delta + \theta - 1$, and hence $d(G) = \delta + \theta$. Now let $\delta^* = \delta_{G,X}(A)$ and $Q = Q_{G,X}(A)$; we have

$$\tilde{P}_{L,\delta^*}(Q, s) = 1 - \frac{q^{\delta^*-1}|\mathrm{Z}^1_Q(L/A, A)|}{q^s}.$$

If $\langle g \rangle \cap \operatorname{soc} G \neq 1$, then $\delta^* < \delta$ and

$$\tilde{P}_{L,\delta^*}(Q, d(G) - 1) = 1 - \frac{|\mathrm{Z}^1_Q(L/A, A)|}{q^{\delta+\theta-\delta^*}} \geqslant 1 - q^{\delta^*-\delta} > 0.$$

If $\langle g \rangle \cap \operatorname{soc} G = 1$, then, since $g \neq 1$, we deduce that Q is a non-trivial subset of $\operatorname{Aut} A$. Hence in particular $\theta = 1$, and moreover $\mathrm{Z}^1_Q(L/A, A) = \{\beta_a \mid a \in C_A(Q)\}$ and $C_A(Q) = 1$, so that $|\mathrm{Z}^1_Q(L/A, A)| = 1$ and

$$\tilde{P}_{L,\delta^*}(Q, d(G) - 1) = 1 - q^{\delta^*-\delta-1} > 0.$$

This concludes the proof.

The previous result does not hold if we drop the hypothesis that G is supersoluble. For example consider the crown-based power $G = (\mathrm{Alt}(4))_2$. It can easily be seen that $d(G) = 2$; moreover $A \in \Omega_G$ if and only if A is G-isomorphic to a minimal normal subgroup of G, and then we have $R_G(A) = 1$. Therefore $\bigcup_{A \in \Omega_G} R_G(A) = 1$. Now let g be a non-trivial element of a minimal normal subgroup M of G. If there exists x such that $G = \langle g, x \rangle$ then $G = \langle M, x \rangle$, and this implies that $G/M \cong \mathrm{Alt}(4)$ is cyclic.

References

[1] M. Aschbacher and R. Guralnick. Some applications of the first cohomology group. *J. Algebra* **90** (1984), 446–460.

[2] N. Boston. A probabilistic generalization of the Riemann zeta functions. In *Analytic number theory*, vol. 1 (Birkhäuser, 1996), pp. 155–162.

[3] H. Crapo. The Möbius function of a lattice. *J. Combinatorial Theory* **1** (1966), 126–134.

[4] F. Dalla Volta and A. Lucchini. Finite groups that need more generators than any proper quotient. *J. Austral. Math. Soc. Ser. A* **64** (1998), 82–91.

[5] E. Detomi and A. Lucchini. Crowns and factorization of the probabilistic zeta function of a finite group. *J. Algebra* **265** (2003), 651–668.
[6] W. Gaschütz. Praefrattinigruppen. *Arch. Math.* (*Basel*) **13** (1962), 418–426.
[7] P. Hall. The Eulerian functions of a group. *Quart. J. Math. Oxford Ser.* **7** (1936), 134–151.
[8] P. Jimenez-Seral and J. Lafuente. On complemented nonabelian chief factors of a finite group. *Israel J. Math.* **106** (1998), 177–188.
[9] A. Mann. Positively finitely generated groups. *Forum Math.* **8** (1996), 429–459.

Received 10 March, 2004

A. Lucchini, Dipartimento di Matematica, Università degli Studi di Brescia, Via Valotti n. 9, 25123 Brescia, Italy
E-mail: lucchini@ing.unibs.it