REND. SEM. MAT. UNIV. PADOVA, Vol. 115 (2006)

On the Dirichlet Polynomial of Finite Groups of Lie Type.

ERIKA DAMIAN (*) - ANDREA LUCCHINI (*)

Dedicated to Guido Zappa on his 90th birthday

ABSTRACT - For a given finite group G there exists a uniquely determined Dirichlet polynomial $P_G(s)$ with the property that for $t \in \mathbb{N}$ the number $P_G(t)$ coincides with the probability of generating G by t randomly chosen elements. We discuss whether the isomorphism type of a simple group G can be determined by the knowledge of $P_G(s)$.

1. Introduction.

For a given finite group G one may define a sequence of integers $\{a_n(G)\}_{n\in\mathbb{N}}$ as follows:

$$a_n(G) = \sum_{|G:H|=n} \mu_G(H).$$

Here μ_G denotes the Möbius function defined on the subgroup lattice of G. In particular, one has $\mu_G(G) = 1$ and $\mu_G(H) = -\sum_{H<K} \mu_G(K)$ for any $H < G$. Let

$$P_G(s) = \sum_{n\in\mathbb{N}} \frac{a_n(G)}{n^s}$$

be the Dirichlet generating function associated with the sequence $\{a_n(G)\}_{n\in\mathbb{N}}$. The Dirichlet polynomial $P_G(s)$ gives a great amount of information about G. In [13] P.Hall observed that for any $t \in \mathbb{N}$ the series $P_G(t)$ gives the probability that t randomly chosen elements of G generate G. Moreover (see for example [3]), the complex function $P_G(s)$, and in

(*) Indirizzo degli AA.: Università di Brescia, Dipartimento di Matematica, Via Valotti, 25133 Brescia, Italy.
E-mail: erika.damian@ing.unibs.it
E-mail: andrea.lucchini@ing.unibs.it

particular its value at -1, can be used to investigate the topological properties of the poset of proper cosets of G.

A problem that has been tackled from various points of view ([10], [9], [6]) concerns the study of which properties of $P_G(s)$, as an element of the ring of Dirichlet polynomials with integer coefficients, reflect on properties of the group G. Recently [8] we proved that the knowledge of $P_G(s)$ allows us to decide whether the factor group G/G is a simple group or not: if G_1 is simple and $P_{G_2}(s) = P_{G_1}(s)$, then $G_2/(G_2)$ is simple. We conjecture that a stronger result is true: if G_1 is simple and $P_{G_2}(s) = P_{G_1}(s)$ then $G_2/G_2 \cong G_1$. This has been proved for alternating simple groups [7], so the aim of this paper is to investigate the case of simple groups of Lie type. The main result we will obtain is that if we know that G is a simple group of Lie type over a field of characteristic p, then with the help of the function $P_G(s)$ we can determine the order of a Sylow p-subgroup of G. This result will be employed to prove that a sporadic simple group can be identified from its Dirichlet polynomial, and also to show that if G_1 and G_2 are non isomorphic simple groups of Lie type defined in the same characteristic, then $P_{G_2}(s) \neq P_{G_1}(s)$.

2. Known results and open questions.

Let G be a finite simple group. We want to discuss about the properties of G that can be deduced from the knowledge of the Dirichlet polynomial $P_G(s)$. The simplest thing to do is to consider the set

$$\upsilon(G) = \{n \in \mathbb{N} \mid a_n(G) \neq 0\}.$$

If $n \in \upsilon(G)$ then G must have a subgroup of index n; moreover the smallest $n \in \upsilon(G)$ with $n > 1$ coincides with $m(G)$, the smallest index of a proper subgroup of G. The main obstacle when we work with $\upsilon(G)$ is that even when we know that G has a subgroup H with index n we are not sure than $n \in \upsilon(G)$; in fact, in order to decide whether $a_n(G) \neq 0$ we should focus on the set of subgroups $H \leq G$ with index n and such that $\mu_G(H) \neq 0$, but here we meet another problem as the sum $a_n(G) = \sum_{|G:H|=n} \mu_G(H)$ can be zero even if the terms are different from zero. A case in which it is easy to deduce that $a_n(G) \neq 0$ is when we know that G has a maximal subgroup of index n and there is no maximal subgroup with index a proper divisor of n (in that case $-a_n(G)$ is precisely the number of maximal subgroups of index n). One can expect that the set $\upsilon(G)$ is large enough to give good hints concerning the order of the group G. Let us formulate two conjectures in this direction. Define the probabilistic order of G as follows:

$$\mathrm{po}(G) = \mathrm{l.c.m.}\{n \mid n \in \upsilon(G)\}$$

Clearly $\mathrm{po}(G)$ divides $|G|$; our first conjecture is that $\mathrm{po}(G) = |G|$; a weaker conjecture is that we can deduce from $\upsilon(G)$ which are the prime divisors of $|G|$, namely: $\pi(\mathrm{po}(G)) = \pi(G)$. Both these conjectures are open questions and it seems a difficult but intriguing task to prove something in this direction without a heavy use of the classification of finite simple groups and of their maximal subgroups.

In [9] and [7] it is proved that an analysis of $\upsilon(G)$ allows to decide whether G is an alternating group; more precisely we have:

THEOREM 1. *Let G be a finite nonabelian simple group. Set $n = m(G)$ and let p be the minimal prime number which divides n;*

(1) *if $n = p$ then: $G \cong \mathrm{Alt}(n)$ if and only if $(n-2)! \in \upsilon(G)$;*

(2) *if $n > p$ and $n \notin \{6{,}24\}$ then: $G \cong \mathrm{Alt}(n)$ if and only if $a_n(G) = -n$ and $\binom{n}{p}$ is the smallest integer in $\upsilon(G)$ which is different from 1 and not divisible by n;*

(3) *if $n = 6$ then: $G \cong \mathrm{Alt}(6)$ if and only if $a_6(G) = -12$;*

(4) *if $n = 24$ then: $G \cong \mathrm{Alt}(24)$ if and only if $253, 759 \notin \upsilon(G)$.*

Hence for the rest of the paper we shall restrict our attention to sporadic simple groups and simple groups of Lie type.

3. Dealing with groups of Lie type.

The problem of recognizing a simple group G from its Dirichlet polynomial $P_G(s)$ is still open. In this section we shall prove a result which turns out to be useful for the analysis of this problem for groups of Lie type. Indeed we shall show that if we know that G is a simple group of Lie type over a field of characteristic p, then we may use the polynomial $P_G(s)$ in order to determine the order of a Sylow p-subgroup of G.

We need to define some other Dirichlet polynomials associated with G and its subgroups.

Let R be the ring of Dirichlet polynomials with integer coefficients; for any finite set of prime numbers π we may define a ring endomorphism of R as follows:

$$\begin{array}{cccc} \eta_\pi : & R & \longrightarrow & R \\ & f(s)=\displaystyle\sum_{n=1}^{\infty}\frac{a_n}{n^s} & \mapsto & f^{(\pi)}(s)=\displaystyle\sum_{n=1}^{\infty}\frac{b_n}{n^s} \end{array}$$

where

$$b_n = \begin{cases} a_n & \text{if } n \text{ is a } \pi^{'}\text{-number} \\ 0 & \text{otherwise.} \end{cases}$$

We are mainly interested in $P_G^{(q)}(s)$, with q a prime number.

Moreover, for any subgroup K of G, we may define a Dirichlet polynomial as follows:

$$P_G(K,s)=\sum_{n\in\mathbb{N}}\frac{a_n(G,K)}{n^s} \quad \text{where} \quad a_n(G,K)=\sum_{\substack{|G:H|=n,\\ K\le H\le G}}\mu_G(H).$$

Lemma 2. *Let P be a Sylow p-subgroup of a finite group G, p a prime number; suppose that each maximal subgroup of G which contains P contains also $N_G(P)$. Then*

$$P_G^{(p)}(s)=P_G(P,s-1)=P_G(N_G(P),s-1).$$

Proof. First we claim that $\mu_G(H)|N_H(P)|=\mu_G(H)|N_G(P)|$ for each subgroup $P\le H\le G$. Indeed, either $\mu_G(H)=0$ or H can be written as intersection of maximal subgroups, say $M_1,\dots,M_t$ (see [14]); as $P\le H\le M_i$, by hypothesis we get that $N_G(P)\le M_i$, which implies $N_G(P)\le M_1\cap\dots\cap M_t=H$ and $N_G(P)=N_H(P)$. Now set $\Omega_p = \{H\le G \mid |H|_p=|G|_p\}$, then

$$\begin{aligned} P_G^{(p)}(s) &= \sum_{H\in\Omega_p}\frac{\mu_G(H)}{|G:H|^s} = \\ &= \sum_{Q\in \mathrm{Syl}_p(G)}\sum_{Q\le H}\frac{\mu_G(H)}{|G:H|^s}\cdot\frac{1}{|H:N_H(Q)|} = \\ &= \frac{1}{|N_G(P)|}\sum_{P\le H}\frac{\mu_G(H)|N_H(P)|}{|G:H|^{s-1}} = \\ &= \frac{1}{|N_G(P)|}\sum_{P\le H}\frac{\mu_G(H)|N_G(P)|}{|G:H|^{s-1}} = \\ &= \sum_{P\le H}\frac{\mu_G(H)}{|G:H|^{s-1}} = P_G(P,s-1). \end{aligned}$$

This proves the first equality in our statement. The other one, $P_G(P, s-1) = P_G(N_G(P), s-1)$, is again an immediate consequence of the previous remark that if $\mu_G(H) \neq 0$ and $P \leq H$, then $N_G(P) \leq H$.

□

THEOREM 3. *Suppose that G is a finite group of Lie type defined over a field of characteristic p and let $U \in \mathrm{Syl}_p(G)$. Then $|P_G^{(p)}(0)| = |U|$.*

PROOF. A finite group G of Lie type over the field $\mathbb{F}_q$, $q = p^f$, can be constructed starting from a connected reductive algebraic group X defined over an algebraically closed field of characteristic p and considering the subgroup $G = X^F$ of fixed points under a Frobenius map F. Let B be an F-stable Borel subgroup of X. The unipotent radical U of B^F is a Sylow p-subgroup of G^F and $N_G(U) = B^F$. As it is well known, a maximal subgroup of G^F which contains U should contain B^F, hence it is a maximal parabolic subgroup of G^F, so we can apply the previous lemma in order to deduce that

$$P_G^{(p)}(0) = P_G(B^F, -1) = \sum_{B^F \leq H} \mu_G(H)|G : H|.$$

To the map F a symmetry ρ on the Dynkin diagram of X is associated (ρ is trivial in the untwisted case). Let $I := \{\mathcal{O}_1, \ldots, \mathcal{O}_k\}$ be the set of the ρ-orbits on the nodes of the Dynkin diagram. If $J \subseteq I$, then $J^* = \bigcup_{j \in J} \mathcal{O}_j$ is a ρ-stable subset of the set of nodes of the Dynkin diagram and one may associate an F-stable parabolic subgroup P_{J^*} of X with J^*. Moreover, the map $J \mapsto P_{J^*}^F$ is an isomorphism between the lattice $\mathcal{P}(I)$ of subsets of I ordered by inclusion, and the lattice of subgroups of G containing B^F. In particular, $\mu_G(P_J) = \mu_{\mathcal{P}(I)}(J) = (-1)^{k-|J|}$ (see [20], 3.8.3). As described in [4], Ch. 9, to any subset J of I, a parabolic subgroup W_J of the Weyl group W^F and a polynomial $P_{W_J}(x)$ are associated with the property that $P_{W_J}(q) = |P_{J^*}^F|$. So one has

$$\begin{aligned} P_G^{(p)}(0) &= \sum_{B^F \leq H} \mu_G(H)|G : H| = \sum_{J \subseteq I} \mu_G(P_{J^*}^F)|G : P_{J^*}^F| \\ &= \sum_{J \subseteq I} (-1)^{k-|J|}|G : P_{J^*}^F| = (-1)^k \sum_{J \subseteq I} (-1)^{|J|} \left(\frac{P_W(q)}{P_{W_J}(q)} \right) \end{aligned}$$

By a theorem of Solomon (see 9.4.5. and Ch. 14 in [4])

$$\sum_{J \subseteq I} (-1)^{|J|} \left(\frac{P_W(q)}{P_{W_J}(q)} \right) = |U|$$

so we conclude that $P_G^{(p)}(0) = (-1)^k |U|$. □

COROLLARY 4. *Let S be a simple group of Lie type defined over a field K; if we know that the characteristic of K is p, then we may determine from the Dirichlet polynomial $P_S(s)$ the order of a Sylow p-subgroup of S.*

PROOF. Let $\mathcal{S} = \{{}^2\mathrm{F}_4(2)', \mathrm{G}_2(2)', {}^2\mathrm{G}_2(3)', \mathrm{B}_2(2)'\}$. If $S \notin \mathcal{S}$ then there exists a finite group of Lie type G with $S = G/Z(G)$; moreover p does not divide $|Z(G)|$ and, by Theorem 3, $P_G^{(p)}(0) = P_S^{(p)}(0)$ is the order of a Sylow p-subgroup of S. On the other hand a direct computation shows that $|P_S^{(p)}(0)| = p|U|$ when $S \in \mathcal{S}$ and U is a Sylow p-subgroup of S. Note that $m(\mathrm{B}_2(2)') = 6$, $m(\mathrm{G}_2(2)') = 28$, $m({}^2\mathrm{G}_2(3)') = 9$, $m({}^2\mathrm{F}_4(2)') = 1600$. Now let S be a simple group of Lie type defined over a field of characteristic p. From the series $P_S(s)$ we recover the value of $m(G)$. If $(p, m(S)) \notin \{(2,6), (2,28), (2,1600), (3,9)\}$, then $S \notin \mathcal{S}$ and $|P_S^{(p)}(0)|$ coincides with the order of the Sylow p-subgroup of S. If $p = 2$ and $m(S) = 28$ then either $S = \mathrm{B}_3(2)$ and $|P_G^{(2)}(0)| = 2^9$ or $S = \mathrm{G}_2(2)'$ and $|P_G^{(2)}(0)| = 2^6$. If $p = 2$ and $m(S) = 1600$ then $G = {}^2\mathrm{F}_4(2)'$; if $p = 2$ and $m(S) = 6$ then $G = \mathrm{B}_2(2)'$; if $p = 3$ and $m(S) = 9$ then $G = {}^2\mathrm{G}_2(3)'$. □

4. Connection between Theorem 3 and the Solomon-Tits Theorem.

In the previous section we proved Theorem 3 by computing directly $P_G(B^F, -1)$, which is possible as we can compute the index and the Möbius function of any parabolic subgroup of G. We would like now to present a different proof for the same result; this is less immediate and direct, but it makes evident the connection between the study of the Dirichlet polynomial $P_G(s)$ and some topological properties of the poset of proper cosets in G.

We first revise and generalize a well-known result of K. S. Brown [3].

Let K be a proper subgroup of a finite group G. We define two posets: the first one, $\mathcal{C} = \mathcal{C}(G, K)$, consists of the proper cosets Hx ($K \le H < G, x \in G$) ordered by inclusion. The second $\mathcal{C}^* = \mathcal{C}^*(G, K)$ is the subposet of $\mathcal{C}$ consisting of the cosets Hx where H satisfies the additional property of being intersection of maximal subgroups of G. As it is well known, we can apply topological concepts to a poset $\mathcal{P}$ by using the simplicial complex $\Delta(\mathcal{P})$ (the order complex of $\mathcal{P}$) whose simplices are the finite chains in $\mathcal{P}$.

LEMMA 5. *The complexes $\Delta(\mathcal{C})$ and $\Delta(\mathcal{C}^*)$ are homotopy equivalent.*

PROOF. We recall the following criterion due to Quillen ([18] Proposition 1.6): if there exists an order preserving map $f : X \to Y$ between two posets, with the property that for any $y \in Y$ the lower fiber $f/y = \{x \in X \mid f(x) \leq y\}$ is contractible, then the complexes $\Delta(X)$ and $\Delta(Y)$ are equivalent. In our case we may define an order preserving map $f : \mathcal{C} \to \mathcal{C}^*$ by sending Ux to $\bar{U}x$, being $\bar{U}$ the intersection of the maximal subgroups of G containing U. For any $Vx \in \mathcal{C}^*$ the lower fiber $f/Vx = \{Uy \mid y \in Vx \text{ and } K \leq U \leq V\}$ is contractible as Vx is a least upper bound for f/Vx. □

If Γ is an n-dimensional complex, the Euler-Poincarè characteristic of Γ is the integer $\chi(\Gamma) = \sum\limits_{0 \leq q \leq n} (-1)^q a_q$, where a_q is the number of q-simplices of Γ. The reduced Euler-Poincarè characteristic is defined as: $\tilde{\chi}(\Gamma) = \chi(\Gamma) - 1$.

Generalizing a result due to Brown in the particular case $K = 1$, we prove that the Euler-Poincarè characteristic of the complexes $\Delta(\mathcal{C})$ and $\Delta(\mathcal{C}^*)$ can be computed with the help of the function $P_G(K, s)$. Indeed one has:

Proposition 6. *$P_G(K, -1) = -\tilde{\chi}(\Delta(\mathcal{C}(G, K))) = -\tilde{\chi}(\Delta(\mathcal{C}^*(G, K)))$.*

Proof. Since $\Delta(\mathcal{C}(G, K))$ and $\Delta(\mathcal{C}^*(G, K))$ are equivalent, it suffices to prove the first equality. Let $\bar{\mathcal{C}}$ be the poset obtained by adding to $\mathcal{C}(G, K)$ a greatest element (which we may well take as G) and a least element (that we denote by 0). Recall that the Möbius function $\mu_{\mathcal{P}}$ associated to a poset $\mathcal{P}$ has the property that if $a < b$ then $\mu_{\mathcal{P}}(a, b)$ is the number of chains of even length in the interval $(a, b) = \{c \in \mathcal{P} \mid a < c < b\}$ minus the number of chains of odd length (here we include the empty chain, which we agree to consider of length -1); this implies that $\mu_P(a, b) = \tilde{\chi}(\Delta(a, b))$. In our particular case we obtain $\mu_{\bar{\mathcal{C}}}(0, G) = \tilde{\chi}(\Delta(\mathcal{C}(G, K))$. Now let $Hx \in \mathcal{C}(G, K)$; the interval $[H, G]$ in the subgroup lattice of G is isomorphic to the interval $[Hx, G]$ in $\bar{\mathcal{C}}$ via the map $U \to Ux$; thus $\mu_{\bar{\mathcal{C}}}(Hx, G) = \mu_G(H)$ and

$$P_G(K, -1) = \sum_{K \leq H \leq G} \mu_G(H)|G : H| = \mu_G(G) + \sum_{Hx \in \mathcal{C}(G,K)} \mu_{\bar{\mathcal{C}}}(Hx, G) =$$

$$= \mu_{\bar{\mathcal{C}}}(G, G) + \sum_{Hx \in \mathcal{C}(G,K)} \mu_{\bar{\mathcal{C}}}(Hx, G) = -\mu_{\bar{\mathcal{C}}}(0, G) = -\tilde{\chi}(\Delta(\mathcal{C}(G, K)).$$

This concludes our proof. □

We shall assume for the remaining part of this section that G is a finite group of Lie type of rank n; as it is well known G admits a (B, N)-pair with B a Borel subgroup of G. Let $\{M_1, \ldots, M_n\}$ be the set of maximal parabolic subgroups of G containing B. The Tits building $\mathcal{T}(G;B,N)$ of G is the simplicial complex whose vertices are the cosets M_ix with $x \in G$ and $1 \leq i \leq n$ and whose simplices are collections of vertices with nonempty intersection. If p is the characteristic of the underlying field of G, then $U = O_p(B)$ is a Sylow p-subgroup of G, and the following holds.

PROPOSITION 7. *The complexes $\Delta(\mathcal{C}(G,U))$ and $\mathcal{T}(G;B,N)$ are homotopy equivalent.*

PROOF. Recall that if $\mathcal{B}$ is a complex, then one can consider the faced poset $P(\mathcal{B})$, consisting of the simplices of $\mathcal{B}$ ordered by inclusion; the order complex $\Delta(P(\mathcal{B}))$ (the first barycentric subdivision of $\mathcal{B}$) is homotopy equivalent to $\mathcal{B}$. Moreover if $\mathcal{P}$ is a poset, then $\Delta(\mathcal{P}) = \Delta(\mathcal{P}^{\mathrm{op}})$, being $\mathcal{P}^{\mathrm{op}}$ the dual poset of $\mathcal{P}$. These remarks together with Lemma 5, implies that our statement is proved if we can show that $\Delta(P(\mathcal{T}(G;B,N)))$ and $\Delta(\mathcal{C}^*(G,U)^{\mathrm{op}})$ are equivalent. By definition an element of $P(\mathcal{T}(G;B,N))$ is a set $\{M_{i_1}x,\dots,M_{i_r}x\}$ with $1 \leq i_1 < \cdots < i_r \leq n$; on the other hand the elements of $\mathcal{C}^*(G,U)$ are cosets Hx where H is intersection of maximal subgroups containing U; since such an H can be written in a unique way as intersection of maximal parabolic subgroups in $\{M_1,\dots,M_n\}$ we obtain that the map $\{M_{i_1}x,\dots,M_{i_r}x\} \mapsto (M_{i_1} \cap \cdots \cap M_{i_r})x$ in an order preserving bijection between the posets $P(\mathcal{T}(G;B,N))$ and $\mathcal{C}^*(G,U)^{\mathrm{op}}$. □

COROLLARY 8. $P_G(U,-1) = -\tilde{\chi}(\mathcal{T}(G;B,N))$.

So we may compute $P_G(U,-1)$ with the help of the celebrated Borel-Tits Theorem [19], which asserts that the Tits building $\mathcal{T}(G;B,N)$ has the homotopy type of a wedge of $|U|$ spheres, each one of dimension $(n-1)$. Since the reduced Euler-Poincarè characteristic of a wedge of t r-dimensional spheres is $(-1)^r t$ we get:

COROLLARY 9. $P_G^{(p)}(0) = P_G(U,-1) = (-1)^n|U|$.

5. Consequences of Theorem 3.

PROPOSITION 10. *If G is a finite simple group of Lie type over a field of characteristic p, then $p \in \pi(\mathrm{po}(G))$.*

PROOF. By Theorem 3, we have that $P_G^{(p)}(0) \neq 0$, while, by the definition of the Möbius function, $P_G(0) = \sum_{H \leq G} \mu_G(H) = 0$. This implies $P_G(s) \neq$

$\neq P_G^{(p)}(s)$, which is possible only when there exists a positive integer n divisible by p with $a_n(G) \neq 0$. □

It is useful to define the following set:

$\tilde{\upsilon}(G)$ is the set of $n \in \mathbb{N}$ with the following property: G contains a maximal subgroup M of index n but it does not contain any proper subgroup H such that $|G : H|$ is a proper divisor of n.

In this section we will make a large use of the following fact (already recalled in section 2): $\tilde{\upsilon}(G) \subseteq \upsilon(G)$.

THEOREM 11. *Let G be a sporadic simple group; if H is a finite simple group with $P_G(s) = P_H(s)$, then $G \cong H$.*

PROOF. By Theorem 1, H cannot be an alternating group. Suppose that $H = L_n(q)$ is a group of Lie type of rank n over a field $\mathbb{F}_q$ of characteristic p; we know that $m(G) = m(H)$, and the possible values for $m(G)$ and $m(H)$ are listed in Table 1; for any family L of groups of Lie type, this table provides a function $f(L, n, q)$ such that $m(L_n(q)) = f(L, n, q)$. So we have to check whether there are some choices of L, n, q for which $f(L, n, q) = m(G)$. The key tool here is that the p-adic expansion of $f(L, n, q)$ is of a very particular and recognizable shape (for example the first and last digits are equal to 1 and the second is 0 or 1); moreover by Proposition 10, $p \in \pi(\mathrm{po}(H)) = \pi(\mathrm{po}(G))$, hence p must be a prime divisor of $|G|$; so what we have to do is to write the p-adic expansion of $m(G)$ for any prime divisor p of $|G|$ and check whether for some choice of L, n, q, with q a p-power, the p-adic expansions of $m(G)$ and of $f(L, n, q)$ are the same. This is almost never the case; in fact there are only two possibilities: $(G, H) \in \{(\mathrm{M}_{11}, \mathrm{A}_1(11)), (\mathrm{M}_{24}, \mathrm{A}_1(23))\}$. In the first case one can check that $\mu_{\mathrm{M}_{11}}(1) \neq 0$, so $|\mathrm{M}_{11}| = 7920 \in \upsilon(\mathrm{M}_{11})$, while $7920 \notin \upsilon(\mathrm{A}_1(11))$ (as 7920 does not divide $|\mathrm{A}_1(11)| = 660$): this is enough to conclude that $P_{\mathrm{M}_{11}}(s) \neq P_{\mathrm{A}_1(11)}(s)$. In the second case, one can notice that $1771 \in \tilde{\upsilon}(\mathrm{M}_{24})$ and does not divide $|\mathrm{A}_1(23)| = 6072$. To conclude our proof it remains to consider the case when G and H are both sporadic simple groups. From Table 1, we have that if G and H are non isomorphic sporadic simple groups with $m(G) = m(H)$, then $\{G, H\} = \{\mathrm{J}_2, \mathrm{HS}\}$. But we can conclude that $P_{\mathrm{J}_2}(s) \neq$ $\neq P_{\mathrm{HS}}(s)$ as $176 \in \tilde{\upsilon}(\mathrm{HS})$ and 176 does not divide $|\mathrm{J}_2|$. □

For the remaining part of this paper our attention will be restricted to finite simple groups of Lie type. It is well known, see [1], [16], that if G and H are non isomorphic simple groups of the same order, then G and H ei-

TABLE 1. Minimal index for sporadic and Lie groups.

G	$m(G)$	G	$m(G)$
M_{11}	11	M_{12}	12
M_{22}	22	M_{23}	23
M_{24}	$3 \cdot 2^3$	J_4	$11^2 \cdot 29 \cdot 31 \cdot 37 \cdot 43$
J_2	$2^2 \cdot 5^2$	J_3	$2^2 \cdot 3^4 \cdot 19$
J_1	$2 \cdot 7 \cdot 19$	Co_1	$2^3 \cdot 3^3 \cdot 5 \cdot 7 \cdot 13$
Co_2	$2^2 \cdot 5^2 \cdot 23$	Co_3	$2^2 \cdot 3 \cdot 23$
Fi_{22}	$2 \cdot 3^3 \cdot 5 \cdot 13$	Fi_{23}	$3^4 \cdot 17 \cdot 23$
Fi'_{24}	$2^3 \cdot 3^3 \cdot 7^2 \cdot 29$	Ly	$2^2 \cdot 3^4 \cdot 11 \cdot 37 \cdot 67$
McL	$5^2 \cdot 11$	He	$2^2 \cdot 3 \cdot 7^3$
Ru	$2^2 \cdot 5 \cdot 7 \cdot 29$	O'N	$2^3 \cdot 3^2 \cdot 5 \cdot 11 \cdot 31$
Suz	$2 \cdot 3^4 \cdot 11$	B	$2^3 \cdot 3^4 \cdot 5^4 \cdot 23 \cdot 31 \cdot 47$
HS	$2^2 \cdot 5^2$	Th	$2^3 \cdot 3^5 \cdot 5^3 \cdot 19 \cdot 31$
HN	$2^5 \cdot 3 \cdot 5^4 \cdot 19$	M	$3^7 \cdot 14^4 \cdot 55 \cdot 65^2 \cdot 29 \cdot 41 \cdot 59 \cdot 71$
$\mathrm{G}_2(3)$	$3^3 \cdot 13$	$\mathrm{A}_1(7)$	7
$\mathrm{G}_2(4)$	$2^5 \cdot 13$	$\mathrm{A}_1(11)$	11
$\mathrm{A}_3(2)$	8	${}^2\mathrm{F}_4(2)'$	$2^6 \cdot 5^2$
$\mathrm{B}_2(3)$	27	${}^2\mathrm{A}_2(5)$	50
$\mathrm{A}_n(q)$	$\dfrac{q^{n+1}-1}{q-1}$	$\mathrm{B}_n(3),\ (n \geq 3)$	$\dfrac{1}{2}3^{n-1}(3^n-1)$
$\mathrm{B}_n(q)$	$\dfrac{q^{2n}-1}{q-1}$	$\mathrm{C}_n(q)$	$\dfrac{q^{2n}-1}{q-1}$
$\mathrm{B}_n(2)$	$2^{n-1}(2^n-1)$	${}^2\mathrm{A}_n(2),\ (6 \mid n+1$	$2^n\dfrac{(2^{n+1}-1)}{3}$
${}^2\mathrm{A}_2(q)$	q^3+1	${}^2\mathrm{A}_3(q)$	$(q+1)(q^3+1)$
$\mathrm{D}_n(q)$	$\dfrac{(q^n+1)(q^{n-1}-1)}{q-1}$	${}^2\mathrm{A}_n(q),\ (n \geq 4)$	$\dfrac{[q^{n+1}-(-1)^{n+1}][q^n-(-1)^n]}{q^2-1}$
${}^2\mathrm{D}_n(q)$	$\dfrac{(q^n+1)(q^{n-1}-1)}{q-1}$	${}^3\mathrm{D}_4(q)$	$(q+1)(q^8+q^4+1)$
$\mathrm{G}_2(q)$	$\dfrac{q^6-1}{q-1}$	$\mathrm{E}_6(q)$	$\dfrac{(q^4+1)(q^9-1)(q^{12}-1)}{(q^3-1)(q-1)}$
${}^2\mathrm{B}_2(q)$	q^2+1	${}^2\mathrm{E}_6(q)$	$\dfrac{(q^4+1)(q^9+1)(q^{12}-1)}{(q^3+1)(q-1)}$
$\mathrm{F}_4(q)$	$\dfrac{(q^4+1)(q^{12}-1)}{q-1}$	${}^2\mathrm{F}_4(q)$	$(q+1)(q^3+1)(q^6+1)$
${}^2\mathrm{G}_2(q)$	q^3+1	$\mathrm{E}_7(q)$	$\dfrac{(q^{14}-1)(q^8-1)(q^{12}-1)}{(q^6-1)(q^4-1)(q-1)}$
$\mathrm{D}_n(2)$	$2^{n-1}(2^n-1)$	$\mathrm{E}_8(q)$	$\dfrac{(q^{10}+1)(q^{16}-1)(q^{24}-1)}{(q^6-1)(q-1)}$

ther are $A_2(4)$ and $A_3(2)$ or are $B_n(q)$ and $C_n(q)$ for some $n \geq 3$ and some odd q. So our task of recognizing a simple group G from its Dirichlet polynomial would be nearly completed if we could determine $|G|$ from $P_G(s)$; however, as we mentioned in Section 2, this is not an easy problem, and it can be tackled only with an intensive use of results on the maximal subgroups of Lie groups. However the following remark is useful and easy to prove.

LEMMA 12. *Let G be a simple group of Lie type and let B be a Borel subgroup. If $|G : B| = u$, then $u \in \upsilon(G)$.*

PROOF. As we noticed in the proof of Theorem 3, $\mu_G(B) = (-1)^l$ where l is the Lie rank in the untwisted case and the number of ρ-orbits on the nodes of the Dynkin diagram in the twisted case. Now suppose $|H| = |B|$ and $\mu_G(H) \neq 0$; as $|G : H| = u$ is coprime with p, the subgroup H contains a Sylow p-subgroup P of G; the normalizer $\bar{B} = N_G(P)$ is again a Borel subgroup and is contained in each maximal subgroup of G which contains P; as H is an intersection of maximal subgroups, $\bar{B} \leq H$, but $|G : \bar{B}| = |G : H| = u$, hence $H = \bar{B}$; as the Borel subgroups in G are all conjugated and self-normalizing, we conclude that $a_u(G) = |G : N_G(B)|\mu_G(B) = (-1)^l u$. □

The previous lemma tells us that the p'-part of $\mathrm{po}(G)$ cannot be too different from $|G|_{p'}$; indeed $|G|_{p'} = |G : B||H|$, being H a Cartan subgroup of the Borel subgroup B, hence $(|G|/\mathrm{po}(G))_{p'}$ divides $|H|$. What is more difficult to understand is how much smaller can $(\mathrm{po}(G))_p$ be compared to $|G|_p$. However, if we already know that p is the characteristic of the Lie group G, then, by Corollary 4, with the help of the Dirichlet polynomial $P_G(s)$ we may compute the number $\mathrm{po}^*(G) = \mathrm{l.c.m.}(|G|_p, \mathrm{po}(G))$, and use this number as a good approximation for $|G|$. For some groups of low rank $(A_1(q), {}^2B_2(q), {}^2A_2(q))$, we will need a more accurate estimate of $\mathrm{po}(G)$. Before starting the analysis of these particular cases, let us recall some definitions and results concerning Zsigmondy primes. A prime number u is called a *primitive prime divisor* of $a^b - 1$ if it divides $a^b - 1$ but it does not divide $a^e - 1$ for any integer $1 \leq e \leq b - 1$. It was proved by Zsigmondy [22] that if a and b are integers greater than 1 and $(a, b) \neq (2, 6)$, then there exists a primitive prime divisor of $a^b - 1$ except when $a = 2$ and b is a Mersenne prime.

LEMMA 13. *The following hold:*

(1) *If $G = A_1(q)$ then $q(q-1)/2$ divides* $\mathrm{po}(G)$;

(2) *if* $G = {}^2B_2(q)$ *then* $q-1$ *divides* $\mathrm{po}(G)$;

(3) *if* $G = {}^2\mathrm{A}_2(q)$ *with* $q = 3^r$ *and* $r > 1$, *then* $(q+1)^2(q-1)$ *divides* $\mathrm{po}(G)$.

Proof. (1) If $G = \mathrm{A}_1(q)$, then looking at the list of its maximal subgroups (see for example [15], Satz 8.27, pag. 213) one can notice the following: if $q \neq 7, 9, 11$, then $G = \mathrm{A}_1(q)$ has a maximal subgroup D isomorphic to the dihedral group of order $2(q+1)/(2, q-1)$ and $|M| = |D|$ for each M maximal subgroup of G with index dividing $|G : D|$ (more precisely either M is conjugate to D or $q = 59$ and $M \cong \mathrm{Alt}\,(5)$); so if $q \neq 7, 9, 11$, then $|G : D| = q(q-1)/2 \in \tilde{\upsilon}(G)$. Finally a direct computation shows that $\mathrm{po}(G) = |G|$ when $G \in \mathrm{A}_1(7)$, $\mathrm{A}_1(9)$, $\mathrm{A}_1(11)$.

(2) If $G = {}^2\mathrm{B}_2(q)$ then $q = 2^e$ with $e \geq 3$ odd; $|G| = q^2(q^2+1)(q-1)$ and the maximal subgroups of G are the following [21]:

(a) B (the parabolic subgroup) with $|B| = q^2(q-1)$;

(b) X_a with $|X_a| = 4(q + a\sqrt{2q} + 1)$ and $a \in \{-1, 1\}$;

(c) $D \simeq \mathrm{D}_{2(q-1)}$ with $|D| = 2(q-1)$;

(d) ${}^2\mathrm{B}_2(q_0)$ where $q = q_0^a$ and a is a prime divisor of e.

Notice that $(q + \sqrt{2q} + 1)(q - \sqrt{2q} + 1) = q^2 + 1$ so there exists $a \in \{-1, 1\}$ such that $|X_a|$ is divisible by a primitive prime divisor u of $2^{4e} - 1$. A maximal subgroup M has order divisible by u only when $M \cong X_a$, hence $|G : X_a| = q^2(q - a\sqrt{2q} + 1)(q-1)/4 \in \tilde{\upsilon}(G)$, and $q-1$ divides $\mathrm{po}(G)$.

(3) For $q = 3^r, r \neq 1, G = {}^2\mathrm{A}_2(q) = \mathrm{PSU}(3, q)$ has order $q^3(q^3+1)(q^2-1)$ and contains the following maximal subgroups [2] (here $\mathbb{Z}_n$ denotes the cyclic group of order n):

(a) $B \cong [q^3] : \mathbb{Z}_{q^2-1}$;

(b) $\mathrm{GU}(2, q)$;

(c) $(\mathbb{Z}_{q+1})^2.\mathrm{Sym}(3)$;

(d) $\mathbb{Z}_{q^2-q+1}.3$;

(e) $\mathrm{PSU}(3, q_0)$ with $q = q_0^a$ and a prime;

(f) $\mathrm{SO}(3, q)$.

Let now u be a primitive prime divisor of $3^{6r} - 1$. If M is a maximal subgroup of G with order divisible by u then M is of the kind described in (d), hence $|G|/(3(q^2 - q + 1)) = q^3(q+1)^2(q-1)/3 \in \tilde{\upsilon}(G)$. □

Now we are ready to start with the proof of our main result.

Theorem 14. *Let* G_1 *and* G_2 *be two simple groups of Lie type defined over fields with the same characteristic; if* $P_{G_1}(s) = P_{G_2}(s)$, *then* $G_1 \cong G_2$.

The proof is quite long and will be splitted in consecutive steps. The main ingredient is an analysis performed in [16], which explains how one can recognize a finite simple group of Lie type from its order. For the convenience of the reader we recall some definitions introduced in [16]. Let $n > 1$ be a natural number, the *contribution* of a prime p to n is the highest power of p dividing n; the following invariants can be defined:

$p(n)$: is called the *dominant prime* in n and it is the prime number whose contribution to n is maximal.

$l(n)$: is the exponent of $p(n)$ so that $p(n)^{l(n)}$ is the largest power of $p(n)$ dividing n.

$\omega(n)$: is the largest order of $p(n)$ modulo a prime divisor p_1 of $n/p(n)^{l(n)}$; such a prime number is called a *prominent prime.*

$\psi(n)$: is the largest order of $p(n)$ modulo a non-prominent prime; one puts $\psi(n) = 0$ in case n has no non-prominent prime divisor other than $p(n)$.

If G is a group of order n than the numbers $p(G) = p(n)$, $l(G) = l(n)$, $\omega(G) = \omega(n)$ and $\psi(G) = \psi(n)$ are called the *Artin invariants* of $|G|$. In [16] the authors prove that apart from few exceptions, there is a unique simple group of Lie type with given values of the Artin invariants. Our first task will be to prove that we can obtain the Artin invariants by looking at the Dirichlet polynomial of the group. From now on, G will be a finite group of Lie type over a field of characteristic p. In general $p(G)$ coincides with the characteristic p of our group of Lie type; indeed we have the following (see [16, Theorem 3.3]):

STEP 1. *Assume that G is a group of Lie type over a field of characteristic p with $G \neq {}^2\mathrm{A}_2(3)$, ${}^2\mathrm{A}_3(2)$; then $p(G) \neq p$ if and only if $m(G)$ is a prime-power with $m(G) > |G|_p$. Moreover one of the following occurs:*

(1) *$m(G)$ is a 2-power, in which case $p = m(G) - 1$ is a Mersenne prime and $G = \mathrm{A}_1(p)$;*

(2) *$m(G)$ is a Fermat prime, in which case $p = 2$ and $G = \mathrm{A}_1(m(G) - 1)$;*

(3) *$m(G) = 9$, in which case $p = 2$ and $G = \mathrm{A}_1(8)$.*

This has the following consequence:

STEP 2. *Let G be a simple group of Lie type defined over a field F; if we know that the characteristic of F is p, then we may determine from the Dirichlet polynomial $P_G(s)$ whether $p(G) = p$ or not, and when $p(G) \neq p$ we may determine G up to isomorphism.*

Proof. First notice that $G = {}^2\mathrm{A}_2(3)$ is the unique simple group of Lie type with $m(G) = 27$; on the other hand $P({}^2\mathrm{A}_3(2)) = 28$ and $G = {}^2\mathrm{A}_3(2)$ is the unique group of Lie type with $m(G) = 28$ and characteristic 2. First notice that $G = {}^2\mathrm{A}_3(2) \simeq \mathrm{B}_2(3)$ is the unique group of Lie type with $m(G) = 27$ (see for example the list of primitive groups of small degree in [11]) so we may recognize G from its Dirichlet polynomial. Next let us consider $G = {}^2\mathrm{A}_2(3)$, here we get $m(G) = 28$ and $p(G) = 2 \neq 3 = p$; if H is a group of Lie type with $m(H) = 28$, then $H \in \{{}^2\mathrm{A}_2(3),\ \mathrm{A}_1(27),\ \mathrm{B}_3(2)\}$. It can be checked (see Lemma 13 and [5]) that $13 \cdot 27 \in \tilde{\upsilon}(\mathrm{A}_1(27))$ and $5 \cdot 24 \in \tilde{\upsilon}(\mathrm{B}_3(2))$ but neither of these numbers divides $|G|$ so if $H \not\simeq G$, then $P_G(s) \neq P_H(s)$.

When $G \notin \{{}^2\mathrm{A}_3(2),\ {}^2\mathrm{A}_2(3)\}$ we proceed as follows: we determine $m(G)$ and $|G|_p$ with the help of the Dirichlet polynomial $P_G(s)$; if $m(G)$ is not a prime-power or $m(G) \leq |G|_p$), then $p = p(G)$; otherwise we are in one of the three cases described in step 1 and in each of them the knowledge of $m(G)$ suffices to determine G up to isomorphism. □

So our theorem is proved when $p(G) \neq p$, and for the rest of the proof our attention will be restricted on groups of Lie type satisfying $p(G) = p$. Clearly, in this case we can obtain also $l(G)$ from the knowledge of $P_G(s)$ as $p^{l(G)} = |G|_p$. Now we start to discuss the other two Artin invariants, $\omega(G)$ and $\psi(G)$. Let us first recall other results from [16]. The order of $G = L(q)$ has a standard factorization:

$$|L(q)| = \frac{1}{d} q^h P(q),$$

where d, h and $P(q)$ are given in [16, Table L1]. In particular (see [16]) this order has the *cyclotomic factorization in terms of* p:

$$|L(q)| = \frac{1}{d} p^l \prod_m \Phi_m(p)^{e_m},$$

where $\Phi_m(x)$ is the m-th cyclotomic polynomial. Let $\alpha(G)$ be the largest value of m for which $e_m \neq 0$ and define $\beta(G)$ as the next largest value of m for which $e_m \neq 0$; as it is explained in [16], a consequence of Zsigmondy's Theorem is that, apart from the few exceptional cases listed in [16] Lemma 4.6, $\alpha(G)$ and $\beta(G)$ coincides with $\omega(G)$ and $\psi(G)$ (and the precise values are reported in [16] Table A.1).

Step 3. *If* $p(G) = p$, *then* $(\omega(G), \psi(G)) = (\omega(\mathrm{po}^*(G)), \psi(\mathrm{po}^*(G)))$.

Proof. As we noticed after the proof of Lemma 12, $|G|/\mathrm{po}^*(G)$ divides the order of a Cartan subgroup H of G. For most cases, in order to prove our statement it will suffice to check that the prime numbers dividing $|H|$ are not relevant when one wants to compute $\omega(G)$ and $\psi(G)$, which is equivalent to verify the following condition:

($*$) *there exist at least two primes u_1 and u_2 which divide $|G|/|H|$ such that the following holds: for any prime u dividing $|H|$, the order of p modulo u is not grater than the order of p modulo u_1 and u_2.*

So before starting with a case by case analysis we recall the value of $|H|$ for the different classes of groups of Lie type. If $G = L_n(q)$ is of untwisted type, then $|H| = (q-1)^n/d$ (see Section 8.6 in [4]); if $G = {}^tL_n(q)$ is a twisted Lie group and all the roots have the same length, then $|H| = \prod_J (q^{|J|} - 1)/d$; where J runs on the set of the ρ-orbits on the nodes of the Dynkin diagram (see Section 14.1 in [4]); if $G \in \{{}^2B_2(q), {}^2G_2(q), {}^2F_4(q)\}$ (i.e. when G has roots of different length), then $|H| = (q-1)^\varepsilon$, with $\varepsilon \in \{1, 2\}$. Now we start with the analysis of the different possibilities; according to [16] Lemma 4.6, there are three cases:

a) $(\omega(G), \psi(G)) = (\alpha(G), \beta(G))$.

In this case the values of $(\omega(G), \psi(G))$ are given in [16] Table A.1. Assume that G is a Lie group over the field $\mathbb{F}_q$ with $q = p^r$; if G is of untwisted type, then any prime u which divides $|H|$, also divides $q-1$, hence p has order at most r modulo u; this means that condition ($*$) is certainly verified when $\omega(G) > \psi(G) > r$ and, by [16] Table A.1, this is true with the only exception of $G = A_1(q)$; in this last case we can easily conclude with the help of Lemma 13. Now assume that G is a twisted Lie group. First consider the cases when all the roots have the same length. If u is a prime divisor of $|H|$, then the order of p modulo u divides $r \cdot s$, with $s = 3$ when $G = {}^3D_4(q)$, and $s = 2$ otherwise. If $G \neq {}^2A_2(q)$, then $\omega(G) > \psi(G) > r \cdot s$ and ($*$) is satisfied. If $G = {}^2A_2(q)$, then $(\omega(G), \psi(G)) = (6r, 2r)$; this information may be recovered from the index of the Borel subgroup B as $|G : B| = q^3 + 1$ is divisible by $\Phi_{6r}(p)\Phi_{2r}(p)$. If $G \in \{{}^2B_2(q), {}^2G_2(q), {}^2F_2(q)\}$, then p has order at most r modulo any prime divisor of $|H| = q - 1$ and condition ($*$) is certainly satisfied except for $G = {}^2B_2(2^r)$ with $r \equiv \pm 1 \bmod 6$. In this last case one can apply Lemma 13 (2).

b) $p = 2$, $\alpha(G) = 6$ or $\beta(G) = 6$.

The pairs $(\omega(G), \psi(G))$ and $(\alpha(G), \beta(G))$ does not coincide when $p = 2$ and either $\alpha(G) = 6$ or $\beta(G) = 6$; there are precisely 18 groups of Lie type in this situation, and the values $(\omega(G), \psi(G))$ for them are given in

[16, Table A.2(a)]; for most of them a direct and easy computation shows that the exist at least two primes u_1 and u_2 dividing the index of the Borel subgroup and such that p has order $\omega(G)$ modulo u_1 and $\psi(G)$ modulo u_2; only two of these groups require more attention. The first of them is $G = \mathrm{A}_2(8)$: in this case $|G| = 2^9 \cdot 3^2 \cdot 7^2 \cdot 73$, $\omega(G) = 9$ is the order of 2 modulo 73 and $\psi(G) = 3$ is the order of 2 modulo 7; but the Borel subgroup B has index $3^2 \cdot 73$, not divisible by 7, so we need to check more carefully whether 7 divides $\mathrm{po}^*(G)$: this can be deduced by looking at the indices of the maximal subgroups, indeed it turns out that $2^9 \cdot 3 \cdot 7^2 \in \tilde{\upsilon}(G)$. A similar situation occurs when $G = {}^2\mathrm{A}_2(8)$: in this case $|G| = 2^9 \cdot 3^4 \cdot 7 \cdot 19$, and $\omega(G) = 18$, $\psi(G) = 3$ are the orders of 2 modulo 19 and 7; 7 does not divide the index of the Borel subgroup but $2^8 \cdot 7 \cdot 19 \in \tilde{\upsilon}(G)$.

c) p is Mersenne, $\beta(G) = 2$, $\psi(G) = 1$ and $G = \mathrm{A}_1(p^2)$, $\mathrm{A}_2(p)$, $\mathrm{B}_2(p)$ or ${}^2\mathrm{A}_2(p)$.

This case does not give us particular problems; same argument which has been applied in case (a) tells us that $\omega(G) = \alpha(G)$ is the order of p modulo a prime divisor of the index of the Borel subgroup B (see [16, Table A.3]). Moreover $|G : B|$ is an even number and $\psi(G) = 1$ is the order of p modulo 2. □

In [16] the authors prove that the are only few pairs of non-isomorphic simple groups of Lie type with the same Artin invariants (the possibilities are listed in [16], Table 5.2). In particular we have:

STEP 4. *Suppose that G_1 and G_2 are two non isomorphic simple groups of Lie type with the same Artin invariants; if $m(G_1) = m(G_2)$ then one of the following occurs:*

(1) $G_1 = {}^2\mathrm{A}_2(q)$, $G_2 = {}^2\mathrm{G}_2(q)$;
(2) $G_1 = {}^2\mathrm{A}_2(q^2)$, $G_2 = {}^2B_2(q^3)$;
(3) $G_1 = \mathrm{A}_1(2^6)$, $G_2 = {}^2\mathrm{A}_2(4)$;
(4) $G_1 = B_n(q)$, $G_2 = \mathrm{C}_n(q)$ *with q odd and $n \geq 3$.*

STEP 5. $P_{{}^2\mathrm{A}_2(q)}(s) \neq P_{{}^2\mathrm{G}_2(q)}(q)$.

PROOF. Assume, by contradiction, that $P_{{}^2\mathrm{A}_2(q)}(s) = P_{{}^2\mathrm{G}_2(q)}(s)$. This would imply $\mathrm{po}({}^2\mathrm{A}_2(q)) = \mathrm{po}({}^2\mathrm{G}_2(q))$; since, by Lemma 13, $(q+1)^2$ divides $\mathrm{po}({}^2\mathrm{A}_2(q))$, we would get that $(q+1)^2$ divides $|{}^2\mathrm{G}_2(q)| = q^3(q^3+1)(q-1)$, which is false. □

Step 6. $P_{{}^2\mathrm{A}_2(q^2)}(s) \neq P_{{}^2B_2(q^3)}(s)$.

Proof. Assume, by contradiction, that $P_{{}^2\mathrm{A}_2(q^2)}(s) = P_{{}^2\mathrm{B}_2(q^3)}(s)$. This would imply $\mathrm{po}({}^2\mathrm{B}_2(q^3)) = \mathrm{po}({}^2\mathrm{A}_2(q^2))$; since, by Lemma 13, $q^3 - 1$ divides $\mathrm{po}({}^2\mathrm{B}_2(q^3))$, we would get that $q^3 - 1$ divides $|{}^2\mathrm{A}_2(q^2)| = q^6(q^6+1)(q^4-1)$, which is false. □

Step 7. $P_{\mathrm{A}_1(2^6)}(s) \neq P_{{}^2\mathrm{A}_2(4)}(s)$.

Proof. Assume by contradiction that $P_{\mathrm{A}_1(2^6)}(s) = P_{{}^2\mathrm{A}_2(4)}(s)$. Thus $\mathrm{po}(\mathrm{A}_1(2^6)) = \mathrm{po}({}^2\mathrm{A}_2(4))$. By Lemma 13 we get that $7 \in \mathrm{po}(\mathrm{A}_1(2^6))$, but $|{}^2\mathrm{A}_2(4)| = 2^6 \cdot 3 \cdot 5^2 \cdot 13$ is not divisible by 7. □

Step 8. *If q is odd and $n \geq 3$. then $P_{B_n(q)}(s) \neq P_{C_n(q)}(s)$.*

Proof. Recall that $|\mathrm{B}_n(q)| = |\mathrm{C}_n(q)| = q^{n^2}\Big(\prod_{1\leq i\leq n}(q^{2i}-1)\Big)/2$. Assume that $q = p^r$ with p an odd prime, and let π be the union of the sets π_1 and π_2, where π_1 is the set of the primitive prime divisors of $p^{2nr}-1$ and π_2 the set of the primitive prime divisors of $p^{(2n-2)r}-1$. Our aim is to prove that $P^{(\pi)}_{\mathrm{B}_n(q)}(s) \neq P^{(\pi)}_{\mathrm{C}_n(q)}(s)$. We will apply a theorem of Feit ([12, Theorem A]) which asserts that if $(2n, q) \notin \{(6,3),(6,5)\}$, then there exists $\bar{u} \in \pi_1$ such that either $\bar{u} > 2nr+1$ or $\bar{u}^2$ divides $p^{2nr}-1 = q^{2n}-1$. By definition, the non trivial contributions to the computation of the Dirichlet polynomial $P^{(\pi)}_G(s)$ come only from the subgroups containing a Sylow u-subgroup of G for each prime $u \in \pi$. The maximal subgroups of $\mathrm{C}_n(q) \cong \mathrm{PSp}\,(2n,q)$ whose order is divisible by at least a prime $u_1 \in \pi_1$ and a prime $u_2 \in \pi_2$ are described in [13] and [17, Table 2.5]. In particular we deduce that if $\mathrm{C}_n(q) \cong \mathrm{PSp}\,(2n,q)$ contains a maximal subgroup M with this property, then $(2n,q) \notin \{(6,3),(6,5)\}$, $r=1$, $u_1 = 2n+1$ and $|M|$ is not divisible by u_1^2; as a consequence we get that $\bar{u} = u_1$ and $\bar{u}^2$ divides $|\mathrm{C}_n(q)|$ whereas $\bar{u}$ does not divide $|M|$. This implies that there is no maximal subgroup of $\mathrm{C}_n(q)$ containing a Sylow u-subgroup for each $u \in \pi$, hence $P^{(\pi)}_{\mathrm{C}_n(q)}(s) = 1$. The situation is different for $\mathrm{B}_n(q) \cong \Omega_{2n+1}(q)$. Indeed if W is a non-singular 1-dimensional subspace of the orthogonal space $V \cong \mathbb{F}_q^{2n+1}$ with the property that $W^\perp$ has type O^-_{2n}, then the stabilizer $M = \mathrm{Stab}_{\Omega_{2n+1}(q)}(W)$ is a maximal subgroup of $\Omega_{2n+1}(q)$ with $|\Omega_{2n+1}(q) : M| = q^n(q^n-1)/2$, a π'-number. This implies $P^{(\pi)}_{\mathrm{B}_n(q)}(s) \neq 1 =$ $= P^{(\pi)}_{\mathrm{C}_n(q)}(s)$. □

6. An example.

The following is the Dirichlet polynomial associated with a finite simple group G; we want to use the results established in the paper in order to identify G up to isomorphism.

$$\begin{aligned} P_G(s)(S) = 1 &- \frac{62}{31^s} + \frac{186}{(2\cdot 3\cdot 31)^s} + \frac{775}{(5^2\cdot 31)^s} - \frac{3100}{(2^2\cdot 5^2\cdot 31)^s} \\ &- \frac{3875}{(5^3\cdot 31)^s} - \frac{4000}{(2^5\cdot 5^3)^s} - \frac{4650}{(2\cdot 3\cdot 5^2\cdot 31)^s} \\ &+ \frac{11625}{(3\cdot 5^3\cdot 31)^s} + \frac{15500}{(2^2\cdot 5^3\cdot 31)^s} + \frac{18600}{(2^3\cdot 3\cdot 5^2\cdot 31)^s} \\ &+ \frac{31000}{(2^3\cdot 5^3\cdot 31)^s} - \frac{186000}{(2^3\cdot 3\cdot 5^3\cdot 31)^s} + \frac{124000}{(2^5\cdot 5^3\cdot 31)^s} \end{aligned}$$

First we notice that $m(G) = 31$; as $a_{31}(G) = -62$, from Theorem 1 we deduce that G is not of alternating type; moreover by Table 1, there is no sporadic simple group H with $m(H) = 31$; hence G is a simple group of Lie type. Now we compute $P_G^{(p)}(0)$ for any prime $p \in \pi(\mathrm{po}(G)) = \{2, 3, 5, 31\}$; we get the following values:

p	2	3	5	31
$P_G^{(p)}(0)$	$2^4 \cdot 23^2$	$3 \cdot 31 \cdot 1723$	5^3	$-3 \cdot 31 \cdot 43$

Only for $p = 5$ the number $|P_G^{(p)}(0)|$ is a p-power, hence by Theorem 3 the Lie group G is defined over a field of characteristic 5, and 5^3 is the order of a Sylow 5-subgroup of G. Moreover $m(G) = 31 \leq |G|_5 = 5^3$ so by the argument in Step 1 of the proof of Theorem 14, $p(G) = 5$ and $l(G) = 3$. The orders of 5 modulo 2,3,31 are, respectively, 1,2,3 so $\omega(G) = 3$ and $\psi(G) = 2$: G has Artin invarians $(p(G), (G), \omega(G), \psi(G)) = (5, 3, 3, 2)$; this allows us to conclude $G \cong \mathrm{A}_2(5) = (3, 5)$.

REFERENCES

[1] E. Artin, *The orders of the classical simple groups.* Comm. Pure Appl. Math., 8 (1955), pp. 455–472.

[2] D. M. Bloom, *The subgroups of PSL(3, q) for odd q.* Trans. Amer. Math. Soc., **127** (1967), pp. 150–178.

[3] K. S. Brown, *The coset poset and probabilistic zeta function of a finite group.* J. Algebra 225, **2** (2000), pp. 989–1012.

[4] R. W. CARTER, *Simple groups of Lie type.* Wiley Classics Library. John Wiley & Sons Inc., New York, 1989. Reprint of the 1972 original, A Wiley-Interscience Publication.

[5] J. H. CONWAY - R. T. CURTIS - S. P. NORTON - R. A. PARKER - R. A. WILSON, *Atlas of finite groups*. Oxford University Press, Eynsham, 1985. Maximal subgroups and ordinary characters for simple groups, With computational assistance from J. G. Thackray.

[6] E. DAMIAN, - A. LUCCHINI, *The Dirichlet polynomial of a finite group and the subgroups of prime power index.* In *Advances in group theory 2002*. Aracne, Rome, 2003, pp. 209–221.

[7] E. DAMIAN - A. LUCCHINI, *Recognizing the alternating groups from their probabilistic zeta function*. Glasgow Math. J., **46** (2004), pp. 595–599.

[8] E. DAMIAN, - A. LUCCHINI, *The probabilistic zeta function of finite simple groups. J. Algebra*, submitted.

[9] E. DAMIAN - A. LUCCHINI - F. MORINI, *Some properties of the probabilistic zeta function on finite simple groups*. Pacific J. Math., **215**, 1 (2004), pp. 3–14.

[10] E. DETOMI - A. LUCCHINI, *Recognizing soluble groups from their probabilistic zeta functions*. Bull. London Math. Soc., **35**, 5 (2003), pp. 659–664.

[11] J. D. DIXON - B. MORTIMER, *Permutation groups, vol.* **163** of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1996.

[12] W. FEIT, *On large Zsigmondy primes*. Proc. Amer. Math. Soc., **102**, 1 (1988), pp. 29–36.

[13] R. GURALNICK - T. PENTTILA - C. E. PRAEGER - J. SAXL, *Linear groups with orders having certain large prime divisors*. Proc. London Math. Soc. (3) **78**, 1 (1999), pp. 167–214.

[14] P. HALL, *The eulerian functions of a group. Quart.* J. Math., **7** (1936), pp. 134-151.

[15] B. HUPPERT, *Endliche Gruppen. I.* Die Grundlehren der Mathematischen Wissenschaften, Band 134. Springer-Verlag, Berlin, 1967.

[16] W. KIMMERLE - R. LYONS - R. SANDLING - D. N. TEAGUE, *Composition factors from the group ring and Artin's theorem on orders of simple groups*. Proc. London Math. Soc. (3) **60**, 1 (1990), pp. 89–122.

[17] M. W. LIEBECK - C. E. PRAEGER - J. SAXL, *The maximal factorizations of the finite simple groups and their automorphism groups*. Mem. Amer. Math. Soc., **86**, (1990), p. 432.

[18] D. QUILLEN, *Homotopy properties of the poset of nontrivial p-subgroups of a group*. Adv. in Math., **28**, 2 (1978), pp. 101–128.

[19] L. SOLOMON, *The Steinberg character of a finite group with BN-pair.* In *Theory of Finite Groups (Symposium, Harvard Univ., Cambridge, Mass., 1968)*. Benjamin, New York, 1969, pp. 213–221.

[20] R. P. STANLEY, *Enumerative combinatorics. Vol. 1*, vol. 49 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1997.

[21] M. SUZUKI, *A class of doubly transitive permutation groups*. In *Proc. Internat. Congr. Mathematicians (Stockholm, 1962)*. Inst. Mittag-Leffler, Djursholm, 1963, pp. 285–287.

[22] K. ZSIGMONDY, *Zur Theorie der Potenzreste*. Monatsh. Math. Phys., **3** (1892), pp. 265–284.

Manoscritto pervenuto in redazione il 7 settembre 2005.