Glasgow Math. J. **46** (2004) 595–599. © 2004 Glasgow Mathematical Journal Trust.
DOI: 10.1017/S0017089504002010. Printed in the United Kingdom

RECOGNIZING THE ALTERNATING GROUPS FROM THEIR PROBABILISTIC ZETA FUNCTION

E. DAMIAN and A. LUCCHINI
Dipartimento di Matematica, Università di Brescia, Via Valotti, 25133 Brescia, Italy
e-mail: damian@ing.unibs.it, lucchini@ing.unibs.it

(Received 1 January, 2004; accepted 4 May, 2004)

Abstract. Let G be a finite group; there exists a uniquely determined Dirichlet polynomial $P_G(s)$ such that if $t \in \mathbb{N}$, then $P_G(t)$ gives the probability of generating G with t randomly chosen elements. We show that if $P_G(s) = P_{\mathrm{Alt}(n)}(s)$, then $G/\operatorname{Frat} G \cong \mathrm{Alt}(n)$.

2000 *Mathematics Subject Classification.* 20P05, 20D06.

1. Introduction. For any finite group G we may define a complex function

$$P_G(s) = \sum_{H \leq G} \frac{\mu_G(H)}{|G:H|^s}.$$

Here $\mu_G(H)$ is the Möbius function defined on the subgroup lattice of G as $\mu_G(G) = 1$ and $\mu_G(H) = -\sum_{H<K} \mu_G(K)$ for any $H < G$. (The multiplicative inverse of $P_G(s)$ was called the probabilistic zeta function in [**2**] and [**11**].) Note that $P_G(s)$ may be rewritten as

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

Hence $P_G(s)$ belongs to the ring of Dirichlet polynomials

$$R := \left\{ \sum_{n=1}^{\infty} \frac{a_n}{n^s} \,\middle|\, a_n \in \mathbb{Z},\ |\{n : a_n \neq 0\}| < \infty \right\}.$$

In [**7**] Hall observed that for any $t \in \mathbb{N}$, $P_G(t)$ is the probability that t randomly chosen elements of G generate the group G.

It is quite natural to investigate what may be recovered about the group G from the complex function $P_G(s)$. Let us first observe that $P_G(s) = P_{G/\operatorname{Frat} G}(s)$ so that the knowledge of the Dirichlet polynomial $P_G(s)$ may give information only about the structure of the factor group $G/\operatorname{Frat} G$. In particular, given two finite groups G_1 and G_2 such that $P_{G_1}(s) = P_{G_2}(s)$, we are interested in comparing $G_1/\operatorname{Frat} G_1$ and $G_2/\operatorname{Frat} G_2$. As was already noted by Gaschütz [**6**], we cannot infer that $G_1/\operatorname{Frat} G_1 \simeq G_2/\operatorname{Frat} G_2$. However in the known counterexamples it turns out that G_1 and G_2 have the same non Frattini chief factors. Thus it seems that a promising conjecture could be the following: let G_1 be a finite simple group and G_2 a finite group such that $P_{G_1}(s) = P_{G_2}(s)$; then $G_2/\operatorname{Frat} G_2 \simeq G_1$. In this paper we prove this conjecture when $G_1 = \mathrm{Alt}(n)$. The case of alternating groups of prime degree was considered in [**4**]; moreover it has been proved that the polynomial $P_{\mathrm{Alt}(n)}(s)$ is irreducible when n is a prime number. It is still an open question whether this result holds for any n.

2. The main theorem. The ring R of Dirichlet polynomials is a factorial domain and an important role in the factorization of $P_G(s)$ in R is played by the normal subgroups of G. We recall a result in this direction that has been employed already in [**4**].

LEMMA 1. *Let G be a finite group and N a normal subgroup of G. Then $P_{G/N}(s)$ divides $P_G(s)$. Moreover, $P_{G/N}(s) = P_G(s)$ if and only if $N \leq \mathrm{Frat}\, G$.*

In order to prove our main theorem we need to state as a lemma a result obtained by Berkovich in [**1**, Theorem 1].

LEMMA 2. *Let Y be a permutation group of degree n. Assume that n is the minimal index of a proper subgroup of Y. Then Y is a simple group.*

THEOREM 3. *Let G be a finite group. Assume that $P_G(s) = P_{\mathrm{Alt}(n)}(s)$ for some $n \geq 5$. Then $G/\mathrm{Frat}\, G \simeq \mathrm{Alt}(n)$.*

Proof. In [**4**] we showed that if n is a prime number, then $P_{\mathrm{Alt}(n)}(s)$ is irreducible and $G/\mathrm{Frat}\, G \simeq \mathrm{Alt}(n)$. Hence we shall assume that n is not a prime number. Note that n is the minimal index of a subgroup of $\mathrm{Alt}(n)$. Thus $a_n(G) = a_n(\mathrm{Alt}(n)) \neq 0$ and if $a_k(G) = a_k(\mathrm{Alt}(n)) \neq 0$, then $k \geq n$. It follows that n is the minimal index of a subgroup of G; hence if $|G : H| = n$, then H is a maximal subgroup, $\mu_G(H) = -1$ and $-a_n(G)$ is the number of these subgroups. Set $Y = G/\mathrm{Core}_G(H)$, where $H \leq G$ is a subgroup of index n.

Note that Y is a primitive permutation group of degree n that satisfies the hypothesis of Lemma 2; hence Y is a simple group. Moreover Y cannot be an abelian simple group, as in this case n is a prime number.

Thus Y is a nonabelian simple group with the following properties:

(P1) n is the minimal index of a proper subgroup of Y;
(P2) $P_Y(s)$ divides $P_{\mathrm{Alt}(n)}(s)$.

The target now is to show that $Y \simeq \mathrm{Alt}(n)$. In fact this implies that $P_{G/\mathrm{Core}_G(H)}(s) = P_{\mathrm{Alt}(n)}(s) = P_G(s)$. Hence, by Lemma 1, we get $\mathrm{Core}_G(H) = \mathrm{Frat}\, G$ and $G/\mathrm{Frat}\, G \simeq \mathrm{Alt}(n)$.

We start by observing that there are only two simple groups with maximal subgroups of index 6, namely Alt(6) and Alt(5); by using (P1) we obtain that for $n = 6$, $Y \simeq \mathrm{Alt}(6)$. Moreover, for $n = 8$ we get that Alt(8) and PSL(2, 7) are the simple groups with maximal subgroups of index 8; since PSL(2, 7) has maximal subgroups of index 7, we get that $Y \simeq \mathrm{Alt}(8)$.

Thus we shall consider $n \geq 9$ and n not a prime number.

Let us first note that by using (P1) we get that $-a_n(Y)$ is the number of subgroups of index n in G containing $\mathrm{Core}_G(H)$. Hence $0 < -a_n(Y) \leq -a_n(G)$. As a consequence, we get $-n = a_n(\mathrm{Alt}(n)) = a_n(G) \leq a_n(Y) < 0$. Furthermore, since Y is a nonabelian simple group, any subgroup of (minimal) index n in Y is self-normalizing. Hence n divides $a_n(Y)$ and $a_n(Y) = a_n(G) = -n$. It follows that

(P3) Y has a unique equivalence class of transitive representations of degree n.

The subgroups of small index in $\mathrm{Alt}(n)$ are known. See Theorem 5.2A of [**5**]. Namely, if $n \geq 9$, $r < n/2$ and $1 < |\mathrm{Alt}(n) : K| < \binom{n}{r}$, then we have three possible cases:

(1) $\mathrm{Alt}(n)_{(\Delta)} \leq K \leq \mathrm{Alt}(n)_{\{\Delta\}}$ with $\Delta \subseteq \{1, \ldots, n\}$ and $|\Delta| < r$;
(2) n is even, $n = 2m$, and $|\mathrm{Alt}(n) : K| = \frac{1}{2}\binom{n}{m}$;
(3) $(n, r, K, |\mathrm{Alt}(n) : K|) = (9, 4, \mathrm{P\Gamma L}(2, 8), 120)$.

Let p be the minimal prime number which divides n. If $1 < |\mathrm{Alt}(n) : K| < \binom{n}{p}$, then K is contained in a stabilizer of a k-set, with $1 \leq k < p$. Indeed if $n > 9$ is even, then $p = 2$ and $\binom{n}{2} < \frac{1}{2}\binom{n}{n/2}$. Hence case (2) does not occur; moreover since $\binom{9}{3} < 120$ case (3) does not occur either. Furthermore if K is contained in a stabilizer of a k-set, with $1 \leq k < p$, then n divides $|\mathrm{Alt}(n) : K|$ whereas n does not divide $\binom{n}{p}$. Hence the subgroups of index $\binom{n}{p}$ (in particular the stabilizers of p-sets) are maximal subgroups of $\mathrm{Alt}(n)$. Hence we get that $a_{\binom{n}{p}}(\mathrm{Alt}(n)) < 0$. Furthermore n divides k whenever $a_k(\mathrm{Alt}(n)) \neq 0$ and $1 < k < \binom{n}{p}$. As a consequence, since Y is a quotient of G, it follows that if $K < Y$ is a subgroup of index $m > 1$ not divisible by n, then there exists $h > 1$ dividing m such that $0 \neq a_h(G) = a_h(\mathrm{Alt}(n))$; hence $m \geq h \geq \binom{n}{p}$. We have the result (P4).

(P4) If $K < Y$ has index $m > 1$ not divisible by n, then $m \geq \binom{n}{p}$, p being the minimal prime number dividing n.

We show that Y is a 2-transitive nonabelian simple group. Assume that this is not the case. Let Γ be the set of p-subsets of $\{1, \ldots, n\}$, where p is the minimal prime number dividing n. Note that the action of Y on Γ is not transitive; that is to say Y is not p-homogeneous. Indeed, by a theorem due to Livingstone and Wagner (1965) and Kantor (1972), (see [**5**, Theorem 9.4B]), a p-homogeneous nonabelian simple group is 2-transitive. As a consequence, there exists an orbit of Y on Γ, say Ψ, with $1 < |\Psi| < \binom{n}{p}$ not divisible by n, but this is in contradiction to (P4).

In order to show that $Y \simeq \mathrm{Alt}(n)$ we shall proceed with a case-by-case analysis of the 2-transitive nonabelian simple groups of degree $n \geq 9$ with a unique equivalence class of representations of degree n, where n is not a prime number. Assume that $Y \not\simeq \mathrm{Alt}(n)$; then Y is in the following list. See [**5**, Section 7.7] as a reference.

n	Condition	Y	No. of actions
$\frac{q^d-1}{q-1}$	$d = 2$	$\mathrm{PSL}(d, q)$	2 if $d > 2$
	$(d, q) \neq (2, 2), (2, 3)$		1 otherwise
$2^{2d-1} + 2^{d-1}$	$d \geq 3$	$\mathrm{Sp}(2d, 2)$	1
$2^{2d-1} - 2^{d-1}$	$d \geq 3$	$\mathrm{Sp}(2d, 2)$	1
$q^3 + 1$	$q \geq 3$	$\mathrm{PSU}(3, q)$	1
$q^2 + 1$	$q = 2^{2d+1} > 2$	$\mathrm{Sz}(q)$	1
$q^3 + 1$	$q = 3^{2d+1} > 3$	$\mathrm{R}(q)$	1
11		$\mathrm{PSL}(2, 11)$	2
11		M_{11}	1
12		M_{11}	1
12		M_{12}	2
15		$\mathrm{Alt}(7)$	2
22		M_{22}	1
23		M_{23}	1
24		M_{24}	1
176		HS	2
276		Co_3	1

https://doi.org/10.1017/S0017089504002010 Published online by Cambridge University Press

Recall that Y is a 2-transitive non abelian simple group of degree n, where $n \geq 9$ is not a prime number and it is the minimal degree of a 2-transitive action of Y. Moreover Y has a unique equivalence class of representations of degree n. As a consequence we may drop from the list the following set of groups: {PSL(2, 11), M_{11} (both actions), M_{12}, Alt(7), M_{23}, HS}. We shall show that the remaining groups in this list, except for M_{24}, have a subgroup of index m not divisible by n such that $m < \binom{n}{2} \leq \binom{n}{p}$, where p is the minimal prime number dividing n. Then we may use (P4) in order to exclude the possibility that Y is one of these.

Indeed, PSL$(2, q)$ has a subgroup of index $m = (n-1)(n-2)/2$. See Satz 8.4 of [**8**, p. 192]. Sz(q) has a subgroup of index $m = \frac{1}{4}(q - r + 1)$, where $r^2 = 2q$. (See [**12**].) $R(q)$ has a subgroup of index $m = q^2(q^2 - q + 1)$. (See [**9**].) M_{22} has a maximal subgroup of index $m = 77$ and Co_3 has a maximal subgroup of index $m = 11178$. (See [**3**].) Moreover, the minimal degree of a 2-transitive representation of Sp$(2d, 2)$ is $n = 2^{d-1}(2^d - 1)$. The other 2-transitive representation of Sp$(2d, 2)$ gives a subgroup of index $m = 2^{d-1}(2^d + 1)$. Finally PSU$(3, q)$ = PGU$(3, q) \cap$ PSL$(3, q^2)$ and so PSU$(3, q)$ has an action on Ω, the set of points of the projective space PG$_2(q^2)$, of degree $t = q^4 + q^2 + 1$ and this action is fixed-point-free. Since $n = 1 + q^3$ does not divide t, it follows that Ω has an orbit of size $1 < k \leq t$ not divisible by n; hence $m = k$.

In order to prove that $Y \not\simeq M_{24}$ we shall show that $P_{M_{24}}(s)$ does not divide $P_{\mathrm{Alt}(24)}(s)$. Then we may conclude by using (P2). Assume that $P_{M_{24}}(s)$ divides $P_{\mathrm{Alt}(24)}(s)$. Let us define for any prime number p an endomorphism α_p in the ring of Dirichlet polynomials R as follows:

$$\alpha_p\left(\sum_n \frac{a_n}{n^s}\right) = \sum_n \frac{b_n}{n^s}, \text{ where } b_n = \begin{cases} 0 & \text{if } p \text{ divides } n, \\ a_n & \text{otherwise.} \end{cases}$$

Since α_p is an endomorphism, for any prime number p we get that $\alpha_p(P_{M_{24}}(s))$ divides $\alpha_p(P_{\mathrm{Alt}(24)}(s))$; we shall reach a contradiction by showing that this is not the case.

Let us first note that there exist two Dirichlet polynomials $P_1(s), P_2(s) \in R$ with $\alpha_{19}(P_1(s)) = P_1(s)$ and $\alpha_{19}(P_2(s)) = P_2(s)$ such that

$$P_{\mathrm{Alt}(24)}(s) = P_1(s) + \frac{1}{19^s} P_2(s).$$

Furthermore, since 19 does not divide the order of M_{24}, then $\alpha_{19}(P_{M_{24}}(s)) = P_{M_{24}}(s)$ and it divides $\alpha_{19}(P_{\mathrm{Alt}(24)}(s)) = P_1(s)$. Moreover $\alpha_2(P_{M_{24}}(s))$ divides $\alpha_2(P_1(s))$. Note that contributions to $\alpha_2(P_1(s))$ are given by subgroups of Alt(24) that contain both a Sylow 2-subgroup and a Sylow 19-subgroup. We claim that Alt(24) does not have proper subgroups containing both a Sylow 2-subgroup and a Sylow 19-subgroup. Indeed let K be such a group. Let $P \leq K$ be a Sylow 2-subgroup of Alt(24); then it contains $x = x_1x_2 \in$ Alt(24), where x_1 and x_2 are two disjoint cycles of length 8 and 16 respectively. Moreover K contains a cycle of length 19. Thus K is a primitive subgroup of Alt(24) and, by Theorem 3.3E in [**5**] we get that K = Alt(24). We conclude that $\alpha_2(P_1(s)) = 1$. Hence $\alpha_2(P_{M_{24}}(s)) = 1$. This contradicts the fact that M_{24} contains a maximal subgroup of odd index. □

REFERENCES

1. Yakov Berkovich, The degree and index of a finite group, *J. Algebra* **214** (1999), 740–761.

2. Nigel Boston, A probabilistic generalization of the Riemann zeta function, in *Analytic number theory, Vol. 1 (Allerton Park, IL, 1995)* Progr. Math. No. 138 (Birhhauser, 1996), 155–162.

3. J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker and R. A. Wilson, *Atlas of finite groups* (Oxford University Press, 1985).

4. Erika Damian, Andrea Lucchini and Fiorenza Morini, Some properties of the probabilistic zeta function of finite simple groups, *Pacific J. Math.*, **251** (2004), 3–14.

5. John D. Dixon and Brian Mortimer, *Permutation groups*, Graduate Texts in Mathematics, Vol. 163 (Springer-Verlag, 1996).

6. Wolfgang Gaschütz, Die Eulersche Funktion endlicher auflösbarer Gruppen, *Illinois J. Math.* **3** (1959), 469–476.

7. Philip Hall, The eulerian functions of a group, *Quart. J. Math. Oxford* **7** (1936), 134–151.

8. B. Huppert, *Endliche Gruppen. I*, Die Grundlehren der Mathematischen Wissenschaften, Band 134 (Springer-Verlag, 1967).

9. Peter B. Kleidman, The maximal subgroups of the Chevalley groups $G_2(q)$ with q odd, the Ree groups ${}^2G_2(q)$, and their automorphism groups, *J. Algebra* **117** (1988), 30–71.

10. Martin W. Liebeck, Cheryl E. Praeger and Jan Saxl, On the O'Nan-Scott theorem for finite primitive permutation groups, *J. Austral. Math. Soc. Ser. A* **44** (1988), no. 3, 389–396.

11. Avinoam Mann, Positively finitely generated groups, *Forum Math.* **8** (1996), no. 4, 429–459.

12. Michio Suzuki, On a class of doubly transitive groups, *Ann. of Math. (2)* **75** (1962), 105–145.