Pacific Journal of Mathematics

THE PROBABILISTIC ZETA FUNCTION OF PSL(2, q), OF THE SUZUKI GROUPS $^2B_2(q)$ AND OF THE REE GROUPS $^2G_2(q)$

MASSIMILIANO PATASSINI

Volume 240 No. 1 March 2009

PACIFIC JOURNAL OF MATHEMATICS
Vol. 240, No. 1, 2009

THE PROBABILISTIC ZETA FUNCTION OF PSL(2, q), OF THE SUZUKI GROUPS $^2B_2(q)$ AND OF THE REE GROUPS $^2G_2(q)$

MASSIMILIANO PATASSINI

We study the Dirichlet polynomial $P_G(s)$ of the groups $G = \mathrm{PSL}(2, q)$, $^2B_2(q)$, and $^2G_2(q)$. For such G we show that if H is a group satisfying $P_H(s) = P_G(s)$, then $H/\mathrm{Frat}(H) \cong G$. We also prove that, when q is not a prime number, $P_G(s)$ is irreducible in the ring of Dirichlet polynomials. Finally, we prove that the coset poset of G is noncontractible.

1. Introduction

Let G be a finite group. We define the Dirichlet polynomial associated to G by

$$P_G(s) = \sum_{n=1}^{\infty} \frac{a_n(G)}{n^s}, \quad \text{where} \quad a_n(G) = \sum_{\substack{H \leq G \\ |G:H|=n}} \mu_G(H).$$

Here $\mu_G : \mathscr{L} \to \mathbb{Z}$ is the Möbius function on the subgroup lattice $\mathscr{L}$ of G, defined inductively by $\mu_G(G) = 1$, $\mu_G(H) = -\sum_{K>H} \mu_G(K)$. In [Hall 1936], it was observed that for any $t \in \mathbb{N}$, the number $P_G(t)$ is the probability that t randomly chosen elements of G generate the group G. The multiplicative inverse $1/P_G(s)$ is called the probabilistic zeta function of G [Boston 1996; Mann 1996].

More generally, let $k \geq 1$ and let $p_1, \ldots, p_k$ be prime numbers. We define the Dirichlet polynomial $P_G^{(p_1,\ldots,p_k)}(s)$ by

$$P_G^{(p_1,\ldots,p_k)}(s) = \sum_{\substack{(n,p_i)=1 \\ \forall i \in \{1,\ldots,k\}}} \frac{a_n(G)}{n^s}.$$

A problem that arises naturally is to determine which properties of the group G are encoded by the polynomial $P_G(s)$. It is known that $P_{G/\mathrm{Frat}(G)}(s) = P_G(s)$ (see Lemma 5), so from the Dirichlet polynomial of G we can only hope to read off properties of $G/\mathrm{Frat}(G)$. Further, it was noted in [Gaschütz 1959] that $P_G(s)$ does not uniquely determine the isomorphism class of $G/\mathrm{Frat}(G)$.

MSC2000: primary 20D30; secondary 20P05, 11M41, 20D06, 20D60, 20E28.

Keywords: probabilistic zeta function, simple Lie groups, Suzuki groups, Ree groups, simple linear groups, coset poset.

Nevertheless, certain group theoretic properties are given by the Dirichlet polynomial. For instance, If G and H are groups such that $P_G(s) = P_H(s)$ and G is soluble (or p-soluble, or perfect), then H has the same property [Damian and Lucchini 2003; Detomi and Lucchini 2003b]. If G is simple and $P_G(s) = P_H(s)$, then $H/\mathrm{Frat}(H)$ is simple [Damian and Lucchini 2007].

Conjecture [Damian et al. 2004]. *If G is simple and $P_G(s) = P_H(s)$, then G is isomorphic to $H/\mathrm{Frat}(H)$.*

This conjecture remains open, but partial results are known. The conjecture holds when G is isomorphic to a simple alternating group [Damian and Lucchini 2004; Damian et al. 2004], to a simple sporadic group [Damian and Lucchini 2006] or to $\mathrm{PSL}(2, p)$ for p prime [Damian et al. 2004]. Similarly:

Theorem 1 [Damian and Lucchini 2006, Theorem 14]. *If G_1 and G_2 are simple groups of Lie type with the same characteristic, then $P_{G_1}(s) = P_{G_2}(s)$ if and only if G_1 is isomorphic to G_2.*

In this paper we prove the conjecture when G is one of the following groups of Lie type: $\mathrm{PSL}(2, q)$, the Suzuki groups ${}^2B_2(q)$ and the Ree groups ${}^2G_2(q)$. More precisely:

Main Theorem. *Suppose G is of the form*

$$\begin{cases} G(q,1) := \mathrm{PSL}(2,q) & \text{with } q = p^f \geq 4,\ p \text{ prime},\ f > 0, \text{ or} \\ G(q,2) := {}^2B_2(q) & \text{with } q = 2^f,\ f > 1 \text{ odd}, \qquad \text{or} \\ G(q,3) := {}^2G_2(q) & \text{with } q = 3^f,\ f > 1 \text{ odd}. \end{cases} \tag{1-1}$$

If H is a group and $P_G(s) = P_H(s)$, then

$$H/\mathrm{Frat}(H) \cong G.$$

For $G = \mathrm{PSL}(2, q)$, with $q \leq 9$, this can be proved directly.

We outline the proof in the complementary case; see Sections 3 and 4 for details. In view of Theorem 1, we need only show that the characteristic p of G can be recovered from the Dirichlet polynomial $P_G(s)$. To do this, we recall from [Damian and Lucchini 2006, Theorem 3] that *if L is a group of Lie type of characteristic p and $X \in \mathrm{Syl}_p(L)$, then $|P_L^{(p)}(0)| = |X|$*. In particular, $P_G^{(p)}(s)$ is a power of p. We show that if t is a prime number different from p, then $P_G^{(t)}(s)$ is not a power of t. Indeed, if t does not divide the order of G, then $P_G^{(t)}(0) = P_G(0) = 0$. Also, if t divides $|G|$, then Propositions 8 and 12 show that $P_G^{(t)}(0)$ is not a power of t. We can now obtain the characteristic of G from the polynomial $P_G(s)$ as the unique prime number r such that $P_G^{(r)}(0)$ is a power of r.

The proof does not use explicit formulas for the Dirichlet polynomials of the groups in question. However, using the results in [Downs 1991], we have computed explicitly the Dirichlet polynomials for PSL(2, q) (see Section 7), and this makes it possible to test directly certain properties one might wonder about. For example, we disprove the following conjecture, proposed in [Damian and Lucchini 2006]:

If G is a finite simple group, then $|G| = \mathrm{lcm}\{n : a_n(G) \neq 0\}$.

A counterexample is provided by $G = \mathrm{PSL}(2, p)$ with $p \equiv \pm 2 \pmod 5$ and $p \equiv 1 \pmod 8$, for which we have $\mathrm{lcm}\{n : a_n(G) \neq 0\} = |G|/2$, according to the list in Section 7.

Further results. We let $\mathcal{R}$ denote the ring of Dirichlet polynomials:

$$\mathcal{R} = \left\{ \sum_{m=1}^{\infty} \frac{a_m}{m^s} : a_m \in \mathbb{Z},\ m \geq 1,\ \left|\{m : a_m \neq 0\}\right| < \infty \right\}.$$

We recall that $\mathcal{R}$ is a factorial domain [Damian et al. 2004]. Also, if G is a finite group, $P_G(s)$ lies in $\mathcal{R}$. Section 5 is devoted to the study of the irreducibility of $P_G(s)$ in $\mathcal{R}$. An important role in the factorization of $P_G(s)$ is played by the normal subgroups of G. In fact, if N is a normal subgroup of G, we define

$$P_{G,N}(s) = \sum_{n=1}^{\infty} \frac{a_n(G,N)}{n^s}, \quad \text{where} \quad a_n(G,N) = \sum_{\substack{|G:H|=n \\ HN=G}} \mu_G(H).$$

Then $P_G(s) = P_{G/N}(s) P_{G,N}(s)$; see [Brown 2000] or [Detomi and Lucchini 2003a]. Now, if G is a group and $P_G(s)$ is irreducible in $\mathcal{R}$, then $G/\mathrm{Frat}(G)$ is simple. But the converse is not true. For example, $P_{\mathrm{PSL}(2,7)}(s)$ is reducible. Moreover, we know from [Damian et al. 2004, Lemma 11, Proposition 14 and 15] that $P_{\mathrm{Alt}_p}(s)$ *is irreducible in $\mathcal{R}$ for any prime number $p \geq 5$, and $P_{\mathrm{PSL}(2,p)}(s)$ is reducible in $\mathcal{R}$ if and only if $p \geq 5$ and $p = 2^e - 1$* (a Mersenne prime) *with* $e \equiv 3 \pmod 4$. (These are the only known examples of finite simple groups whose Dirichlet polynomial is reducible.) We will prove:

Proposition 2. *If G is as in the Main Theorem and is not isomorphic to* PSL(2, p) *for $p = 2^e - 1$,* $e \equiv 3 \pmod 4$, *then $P_G(s)$ is irreducible in $\mathcal{R}$.*

In Section 6 we study the topological interpretation of the value $P_G(-1)$ proposed in [Brown 2000]. Given a finite group G, we define the simplicial complex Δ, where the simplices of Δ are finite chains of the coset poset of G. If Δ is contractible, its reduced Euler characteristic $\tilde{\chi}(\Delta) := \chi(\Delta) - 1$ is zero. Brown showed that the number $\tilde{\chi}(\Delta)$ is equal to $-P_G(-1)$. Hence, if $P_G(-1) \neq 0$, the simplicial complex associated to the group G is not contractible. Brown also proved that $P_G(-1)$ is nonzero for a soluble group G and conjectured that $P_G(-1)$ is nonzero for every finite group G. At the time of this writing, there is no known finite group G such that $P_G(-1) = 0$. In Section 6 we prove:

Proposition 3. *If G is as in the Main Theorem, then $P_G(-1) \neq 0$.*

2. Some lemmas

Lemma 4 [Zsigmondy 1892]. *Let $a, n \geq 2$ be integers, and assume it is not the case that*

$$n = 2,\ a = 2^s - 1 \text{ with } s \geq 2 \quad \text{or} \quad n = 6,\ a = 2.$$

Then there exists a prime divisor q of $a^n - 1$ such that q does not divide $a^i - 1$ for any i satisfying $0 < i < n$. Such a divisor is called a ***Zsigmondy prime for*** $\langle a, n \rangle$.

We will use repeatedly, often without mention, the following results on the Möbius function of the subgroup lattice of G.

Lemma 5 [Hall 1936]. *Let G be a finite group and H a subgroup of G. If $\mu_G(H)$ does not vanish, H is an intersection of maximal subgroups of G.*

Lemma 6 [Hawkes et al. 1989, Theorem 4.5]. *Let G be a finite group and H a subgroup of G. The index $|N_G(H) : H|$ divides $\mu_G(H)|G : HG'|$.*

If G is perfect, that is, if $G = G'$, Lemma 6 says that $\mu_G(H)\big|G : N_G(H)\big|$ is divisible by $|G : H|$.

Notation. *Throughout the paper, p is a prime number, f is a positive integer, and $q := p^f$ is at least 4.*

3. $P_G^{(t)}(0)$ for the projective linear group $G = \mathrm{PSL}(2, q)$

In this section, assume $G = \mathrm{PSL}(2, q)$ and define $\delta = \gcd(q-1, 2)$.

Theorem 7 [Huppert 1967, p. 213]. *Let $q \geq 5$. If M is a maximal subgroup of* $\mathrm{PSL}(2, q)$, *then M is isomorphic to one of the following groups*:

(1) $C_p^f \rtimes C_{(q-1)/\delta}$;

(2) $D_{2(q-1)/\delta} = N_G(C_{2(q-1)/\delta})$, *for* $q \notin \{5, 7, 9, 11\}$;

(3) $D_{2(q+1)/\delta} = N_G(C_{2(q+1)/\delta})$, *for* $q \notin \{7, 9\}$;

(4) $\mathrm{PGL}(2, q_0)$, *for* $q = q_0^2$, $q_0 \neq 2$;

(5) $\mathrm{PSL}(2, q_0)$, *for* $q = q_0^r$, $q_0 \neq 2$ *where r is an odd prime*;

(6) A_5, *for $p \neq 2$ and $q = p$ or p^2. If $q = p$, then* $q \equiv \pm 1 \pmod 5$ *and if $q = p^2$, then* $p \equiv \pm 3 \pmod 5$;

(7) A_4, *for* $q = p \equiv \pm 3 \pmod 8$ *and* $q \not\equiv \pm 1 \pmod 5$;

(8) S_4, *for* $q = p \equiv \pm 1 \pmod 8$.

Proposition 8. *Let t be a prime number dividing the order of G. If $t \neq p$, then $|P_G^{(t)}(0)|$ is a power of t if and only if*

$$(q, t) \in \{(4, 5), (5, 2), (7, 2), (8, 3), (9, 2), (9, 5)\}.$$

If $t = p$, then $P_G^{(t)}(0) = -q$.

Proof. If $q \leq 11$ or $q+1$ divides 120, the proposition holds by direct inspection; here are the corresponding values of $P_G^{(t)}(0)$.

q	$t=$ 2	3	5	7	11	19	23	29	59
4	−4	6	**−5**	0	0	0	0	0	0
5	**−4**	6	−5	0	0	0	0	0	0
7	**8**	63	0	−7	0	0	0	0	0
8	−8	**−27**	0	28	0	0	0	0	0
9	**16**	−9	**25**	0	0	0	0	0	0
11	144	−21	165	0	−11	0	0	0	0
19	856	171	500	0	0	−19	0	0	0
23	760	1266	0	0	253	0	−23	0	0
29	3220	204	1625	406	0	0	0	−29	0
59	29088	3423	15400	0	0	0	0	1711	−59

For the rest of the proof, assume $q > 11$ and $q+1 \nmid 120$. Let $\mathscr{C}$ be a set of representatives of the conjugacy classes of subgroups of G. Set

(3-1) $$\mathscr{A}_t = \{K \in \mathscr{C} : (|G:K|, t) = 1, \mu_G(K) \neq 0\}.$$

By definition,

$$P_G^{(t)}(s) = \sum_{K \in \mathscr{A}_t} \frac{\mu_G(K)\,|G:N_G(K)|}{|G:K|^s}.$$

(1) *First consider the case $t = p$.* Let Q be a Sylow p-subgroup of G. Since $|Q| = q$, Theorem 7 yields that Q is contained in a maximal subgroup M of G isomorphic to $C_p^f \rtimes C_{(q-1)/\delta}$. Therefore, $Q \cong C_p^f$ and $N_G(Q) = M$. Hence Q is contained in a unique maximal subgroup of G. Therefore we have

(3-2) $$P_G^{(p)}(s) = 1 - \frac{q+1}{(q+1)^s},$$

and hence $P_G^{(p)}(0) = -q$.

(2) *Next consider the case where t divides $(q+1)/\delta$.* Let $\mathscr{D}_t$ be the subset of $\mathscr{A}_t$ consisting of G and of the maximal subgroups of G isomorphic to $D_{2(q+1)/\delta}$. Set $\mathscr{B}_t = \mathscr{A}_t - \mathscr{D}_t$. Using the equality $1 - q(q-1)/2 = (q+1)(2-q)/2$, we have

$$P_G^{(t)}(0) = \frac{(q+1)(2-q)}{2} + \sum_{K \in \mathscr{B}_t} \mu_G(K)\,|G:N_G(K)|.$$

Now let K be in $\mathcal{B}_t$. By Theorem 7, K is contained in a maximal subgroup M isomorphic to one of $D_{2(q+1)/\delta}$, A_5, A_4, S_4, $\mathrm{PSL}(2, q_0)$, $\mathrm{PGL}(2, q_0)$ for some q_0.

We claim that if K is the intersection of two distinct maximal subgroups M_1 and M_2 isomorphic to $D_{2(q+1)/\delta}$, then K is contained in a maximal subgroup of G not isomorphic to $D_{2(q+1)/\delta}$. Indeed, for each divisor $d > 2$ of $(q+1)/\delta$, there exists a unique cyclic subgroup C_d of order d in M_1. Hence C_d is normal, so it is contained in a unique maximal subgroup of G, i.e., M_1. Thus, by the structure of the subgroup lattice of dihedral groups, either $|M_1 \cap M_2| \le 2$ or $M_1 \cap M_2$ is a Klein four-group. In the former case, $M_1 \cap M_2$ is not contained in $\mathcal{B}_t$, since the index of $M_1 \cap M_2$ in G is divisible by $(q+1)/\delta$. In the latter case, the normalizer in G of the Klein four-group $M_1 \cap M_2$ is either A_4 or S_4 [Huppert 1967, 8.16–8.17, Hilfssatz]. Hence $K = M_1 \cap M_2$ is contained in a maximal subgroup of G not isomorphic to $D_{2(q+1)/\delta}$.

Suppose that q is a Mersenne prime greater than or equal to 31. By its definition, $\mathcal{B}_t$ is empty. Therefore $P_G^{(2)}(0)$ equals $(q+1)(2-q)/2$, which is not a power of 2.

Suppose that q is not a Mersenne prime. We claim there exists a prime divisor z of $(q+1)/\delta$, depending on t, such that if K lies in $\mathcal{B}_t$, then z divides $|G:K|$. Before proving our claim, we conclude the proof of the proposition in the current case (2). By Lemma 6, the prime z divides $P_G^{(t)}(0)$. Hence, if $z \neq t$, then $P_G^{(t)}(0)$ is not a power of t. Further, if $z = t$, then $\mathcal{B}_t = \varnothing$ and so $P_G^{(t)}(0) = (q+1)(2-q)/2$ is not a power of t.

It remains to prove our claim. We consider two subcases.

(a) *$\mathcal{B}_t$ contains a maximal subgroup of G isomorphic to A_4, A_5 or S_4.* Then Theorem 7 implies that f is either 1 or 2, and $\mathcal{B}_t$ does not contain any maximal subgroup isomorphic to $\mathrm{PSL}(2, q_0)$. We define the prime number z as follows:

if 2^4 divides $q+1$, let $z = 2$;
otherwise if 3^2 divides $q+1$, let $z = 3$;
otherwise if 5^2 divides $q+1$, let $z = 5$;
otherwise let z be a Zsigmondy prime for $\langle p, 2f\rangle$ distinct from 3 and 5.

This is possible. Indeed, if $2^4 \nmid q+1$, $3^2 \nmid q+1$ and $5^2 \nmid q+1$, then $q+1$ divides $2^3 \cdot 3 \cdot 5 \cdot m$ for some natural number m. Since we are assuming that $q+1$ does not divide 120, we have $(m, 120) = 1$. So there exists a Zsigmondy prime as required.

We claim that, if $K \in \mathcal{B}_t$, then z divides $|G:K|$. This is clear if K is contained in maximal subgroup isomorphic to A_4, A_5 or S_4. Now, suppose that $\mathcal{B}_t$ contains a subgroup M isomorphic to $\mathrm{PGL}(2, p)$, $q = p^2$. In this case, z is greater than 2. Indeed, if $z = 2$, then 2^4 divides $q+1$, so q is not a square, a contradiction. If $z > 2$, then z is a Zsigmondy prime for $\langle p, 2f\rangle$, so z divides $|G:M|$.

(b) *$\mathcal{B}_t$ does not contain a maximal subgroup of G isomorphic to A_4, A_5 or S_4.* Choose z as a Zsigmondy prime for $\langle p, 2f\rangle$. Clearly, z divides $|G:K|$ if $K \in \mathcal{B}_t$.

(3) We now turn to the remaining case, namely, t *divides* $(q-1)/\delta$. Let $\mathcal{D}_t$ be the subset of $\mathcal{A}_t$ consisting of G and of the maximal subgroups of G isomorphic to $C_p^f \rtimes C_{(p-1)/\delta}$. Set $\mathcal{B}_t = \mathcal{A}_t - \mathcal{D}_t$. We have

$$P_G^{(t)}(0) = 1 - (q+1) + \sum_{K \in \mathcal{B}_t} \mu_G(K)\,\big|G : N_G(K)\big| = -q + \sum_{K \in \mathcal{B}_t} \mu_G(K)\,\big|G : N_G(K)\big|.$$

By Theorem 7, if $K \in \mathcal{B}_t$, then K does not contain a Sylow p-subgroup Q of G. Indeed, Q is contained in a unique maximal subgroup isomorphic to $C_p^f \rtimes C_{(p-1)/\delta}$. Hence, p divides $|G : K|$. By Lemma 6, p divides $P_G^{(t)}(0)$. □

4. $P_G^{(t)}(0)$ for the Suzuki and Ree groups

In this section f is odd and greater than 1, p is either 2 or 3, and $G = G(q, p)$ in the notation of the Main Theorem; that is, G is either the Suzuki group ${}^2B_2(q)$ or the Ree group ${}^2G_2(q)$. The order of G is $q^p(q^p+1)(q-1)$.

Define $\alpha_q^{(\pm)} = q \pm \sqrt{pq} + 1$. Note that $\gcd(\alpha_q^{(+)}, \alpha_q^{(-)}) = 1$ and $\alpha_q^{(+)}\alpha_q^{(-)} = \Phi_{2p}(q)$, where $\Phi_4(s) = s^2 + 1$ and $\Phi_6(s) = s^2 - s + 1$.

Lemma 9. *Let $p^\beta p_1^{\beta_1} \cdots p_n^{\beta_n}$ be a prime factorization of f, where $p_i > p$, $\beta_i \geq 1$ for $i \in \{1, \dots, n\}$, and $\beta \geq 0$. We have*

$$\gcd\left(\frac{\Phi_{2p}(q)}{\Phi_{2p}(s_1)}, \dots, \frac{\Phi_{2p}(q)}{\Phi_{2p}(s_n)}, \alpha_q^{(\pm)}\right) > 1,$$

where $s_i^{p_i} = q$ for $i \in \{1, \dots, n\}$.

Proof. Since f is odd, $\beta = 0$ if $p = 2$.

Let $k \leq n$, $1 \leq i_1 < \cdots < i_k \leq n$ and $s_{i_1,\dots,i_k} = p^{f/(p_{i_1}\cdots p_{i_k})}$. Note that

$$\gcd\big(\Phi_{2p}(s_{i_1}), \dots, \Phi_{2p}(s_{i_k})\big) = \Phi_{2p}(s_{i_1,\dots,i_k})$$

and

$$\Phi_{2p}^{(\pm)}(s_{i_1,\dots,i_k}) = \gcd\big(\Phi_{2p}(s_{i_1,\dots,i_k}), \alpha_q^{(\pm)}\big) \in \big\{\alpha^{(+)}_{s_{i_1,\dots,i_k}}, \alpha^{(-)}_{s_{i_1,\dots,i_k}}\big\}.$$

Observe also that $\dfrac{s_{i_1,\dots,i_k}}{p} < \Phi_{2p}^{(\pm)}(s_{i_1,\dots,i_k}) < p\, s_{i_1,\dots,i_k}$. So we have

$$\prod_{k=1}^{n}\Bigg(\prod_{1\leq i_1<\cdots<i_k\leq n} \Phi_{2p}^{(\pm)}(s_{i_1,\dots,i_k})\Bigg)^{(-1)^{k+1}} < \prod_{k=1}^{n}\Bigg(\prod_{1\leq i_1<\cdots<i_k\leq n} p^{(-1)^{k+1}} s_{i_1,\dots,i_k}\Bigg)^{(-1)^{k+1}} \leq p^{f-1} < \alpha_q^{(\pm)},$$

where for the second inequality we use that $p_i - 1 \geq p$ for all i in $\{1, \dots, n\}$. Now the lemma follows from this equality, whose verification is left to the reader:

$$\gcd\left(\frac{\Phi_{2p}(q)}{\Phi_{2p}(s_1)}, \dots, \frac{\Phi_{2p}(q)}{\Phi_{2p}(s_n)}, \alpha_q^{(\pm)}\right)\prod_{k=1}^{n}\Bigg(\prod_{1\leq i_1<\cdots<i_k\leq n} \Phi_{2p}^{(\pm)}(s_{i_1,\dots,i_k})\Bigg)^{(-1)^{k+1}} = \alpha_q^{(\pm)}.$$

□

Theorem 10 [Suzuki 1962]. *Let $p=2$. Any maximal subgroup of $G={}^2B_2(q)$ is isomorphic to one of the following groups*:

(1) $H=Q\rtimes W$, *where Q is a Sylow 2-subgroup of G and W is a cyclic group of order $q-1$*;

(2) $B_0=N_G(W)$, *a dihedral group of order $2(q-1)$*;

(3) $B_+=A_+\rtimes C_4$, *where A_+ is a cyclic group of order $\alpha_q^{(+)}=q+\sqrt{2q}+1$*;

(4) $B_-=A_-\rtimes C_4$, *where A_- is a cyclic group of order $\alpha_q^{(-)}=q-\sqrt{2q}+1$*;

(5) ${}^2B_2(s)$, *where $q=s^r$ for some prime number r*.

Theorem 11 [Kleidman 1988]. *Let $p=3$. Any maximal subgroup of $G={}^2G_2(q)$ is isomorphic to one of the following groups*:

(1) $H=Q\rtimes C_{q-1}$, *where Q is a Sylow 3-subgroup of G*;

(2) $B=C_G(i)$, *where i is an involution of G. Furthermore*, $B\cong\langle i\rangle\times \mathrm{PSL}(2,q)$;

(3) $B_0=N_G(\langle i,j\rangle)$, *with $\langle i,j\rangle\cong C_2\times C_2$. Moreover*, $B_0\cong(C_2\times C_2\times D_{(q+1)/2})\rtimes C_3$ *has order* $6(q+1)$;

(4) $B_+=A_+\rtimes C_6$, *where A_+ is a cyclic group of order $\alpha_q^{(+)}=q+\sqrt{3q}+1$*;

(5) $B_-=A_-\rtimes C_6$, *where A_- is a cyclic group of order $\alpha_q^{(-)}=q-\sqrt{3q}+1$*;

(6) ${}^2G_2(s)$, *where $q=s^r$ for some prime number r*.

Proposition 12. *Let t be a prime number dividing the order of G. If $t\neq p$, then $|P_G^{(t)}(0)|$ is not a power of t. If $t=p$, then $P_G^{(t)}(0)=-q^p$.*

Proof. Let $\mathscr{A}_t$ be defined as in (3-1). We partition the proof into four cases.

(1) *Assume that $t=p$.* Let Q be a Sylow p-subgroup of G. Since $|Q|=q^p$, Theorems 10 and 11 show that Q is contained in a unique maximal subgroup isomorphic to H. Hence

$$P_G^{(p)}(0)=\sum_{K\in\mathscr{A}_p}\mu_G(K)\big|G:N_G(K)\big|=1-(1+q^p)=-q^p.$$

(2) *Assume that $t\,|\,q+1$ and $p=3$.* Let r be a Zsigmondy prime for $\langle 3,f\rangle$. Note that $r\neq t$. Let $\mathscr{B}_t$ be the subset of $\mathscr{A}_t$ consisting of the subgroups K of G such that r divides $|G:K|$.

By Theorem 11, if $K\in\mathscr{A}_t-\mathscr{B}_t$ and $K\neq G$, every maximal subgroup containing K is isomorphic to B. We claim that if $K\in\mathscr{A}_t-\mathscr{B}_t$ and $K\neq G$, then K is a maximal subgroup isomorphic to B. Indeed, assume that K is contained in the intersection of M_1 and M_2, two distinct maximal subgroups of G isomorphic to B. Since $M_1\cong\mathrm{PSL}(2,q)\times C_2$, the intersection $M_1\cap M_2$ is isomorphic to a subgroup L of $\mathrm{PSL}(2,q)\times C_2$. Let $\pi:\mathrm{PSL}(2,q)\times C_2\to\mathrm{PSL}(2,q)$ be the projection on the first factor. If $\pi(L)=\mathrm{PSL}(2,q)$, we have $|M_2:M_1\cap M_2|=|M_1:M_1\cap M_2|=$

$|\mathrm{PSL}(2,q)\times C_2 : L| \le 2$; hence $M_1\cap M_2$ is normalized by M_1 and M_2, a contradiction. If $\pi(L) < \mathrm{PSL}(2,q)$, then there exists a maximal subgroup J of $\mathrm{PSL}(2,q)$ containing $\pi(L)$. By Theorem 7, since $q = 3^f$ and $f \ge 3$ is odd, $|\mathrm{PSL}(2,q) : J|$ is divisible by r or t. Since $|L| \le 2|J|$, the index $|\mathrm{PSL}(2,q) : J|$ divides $|G : M_1\cap M_2|$. Hence $|G : M_1 \cap M_2|$ is divisible by r or t, against the assumption $K \in \mathcal{A}_t - \mathcal{B}_t$.

This shows that

$$P_G^{(t)}(0) = 1 - q^2(q^2-q+1) + \sum_{K\in\mathcal{B}_t} \mu_G(K)\,\big|G : N_G(K)\big|$$
$$\equiv -(q-1)(q^3+q+1) \equiv 0 \pmod{r},$$

so $P_G^{(t)}(0)$ is not a power of t.

(3) *Assume that* $t \mid q-1$ *and* $t \ne 2$. Let $\mathcal{D}_t$ be the subset of $\mathcal{A}_t$ consisting of G and of the maximal subgroups of G isomorphic to H. Set $\mathcal{B}_t = \mathcal{A}_t - \mathcal{D}_t$. We have

$$P_G^{(t)}(0) = 1-(q^p+1)+\sum_{K\in\mathcal{B}_t} \mu_G(K)\,\big|G : N_G(K)\big| = -q^p + \sum_{K\in\mathcal{B}_t} \mu_G(K)\,\big|G : N_G(K)\big|.$$

By Theorems 10 and 11, if $K \in \mathcal{B}_t$, then K does not contain a Sylow p-subgroup Q of G. Indeed, Q is contained in a unique maximal subgroup isomorphic to H. Hence, p divides $|G : K|$. By Lemma 6, we obtain that p divides $P_G^{(t)}(0)$.

(4) *Finally, assume that* $t \mid \Phi_{2p}(q)$. Then $t \mid \alpha_q^{(\pm)}$ (that is, $t \mid \alpha_q^{(+)}$ or $t \mid \alpha_q^{(-)}$). Let K be in $\mathcal{A}_t$. By Theorems 10 and 11, if $K \ne G$, then K is contained in a maximal subgroup isomorphic either to $B_\pm$ or to $G(s)$, where $s^r = q$ for some prime number r.

We claim that K is not contained in the intersection of two distinct maximal subgroups M_1 and M_2 isomorphic to $B_\pm$. Indeed, for each divisor $d \ne 1$ of $\alpha_q^{(\pm)}$, there exists a unique subgroup L of M_1 of order d. Hence L is normal in M_1. Therefore M_1 is the unique maximal subgroup of G containing L. So L is not a subgroup of $M_1 \cap M_2$. Thus, d divides $|G : M_1 \cap M_2|$. Thence $|G : M_1 \cap M_2|$ is divisible by $\alpha_q^{(\pm)}$. Since t divides $\alpha_q^{(\pm)}$ and K lies in $\mathcal{A}_t$, we obtain the claim.

Let $\mathcal{D}_t$ be the subset of $\mathcal{A}_t$ consisting of G and of the maximal subgroups of G isomorphic to $B_\pm$. Set $\mathcal{B}_t = \mathcal{A}_t - \mathcal{D}_t$. We have

$$P_G^{(t)}(0) = 1 - \frac{q^p\alpha_q^{(\mp)}(q^{p-1}-1)}{2p} + \sum_{K\in\mathcal{B}_t} \mu_G(K)\,\big|G : N_G(K)\big|.$$

Observe that $\alpha_q^{(\pm)}$ divides $1-q^p\alpha_q^{(\mp)}(q^{p-1}-1)/(2p)$. Moreover, for each $K \in \mathcal{B}_t$, there exists a number s (where $s^r = q$ for some prime number r) such that K is contained in a maximal subgroup M isomorphic to $G(s)$. Let $\mathcal{S}_t$ be the subset of the natural numbers consisting of all such s:

$$\mathcal{S}_t = \big\{ s \in \mathbb{N} : s^r = q,\ r \text{ prime},\ \exists K \in \mathcal{B}_t \text{ such that } K \le G(s)\big\}.$$

Suppose that $\mathcal{S}_t = \{s_1, \ldots, s_k\}$ for some $k \geq 1$. Let $p^{\beta} p_1^{\beta_1} \cdots p_n^{\beta_n}$ be a prime factorization of f, where $p_i > p$, $\beta_i \geq 1$ for $i \in \{1, \ldots, n\}$ and $\beta \geq 0$. Note that

$$\mathcal{S}_t \subseteq \{s \in \mathbb{N} : s^{p_i} = q, \text{for some } i \in \{1, \ldots, n\}\}.$$

Clearly, if $s \in \mathcal{S}_t$, then $s^u = q$ for some prime u dividing f. Moreover, since f is odd, if $p = 2$, then $u \neq 2$. If $p = 3$, then $s = 3^{f/3}$ does not lie in $\mathcal{S}_t$. In fact, if $K \leq G(s)$, then $\Phi_6(q)$ divides $|G:K|$ and so $K \notin \mathcal{B}_t$. By Lemma 9, there exists a prime divisor r of

$$\gcd\left(\frac{\Phi_{2p}(q)}{\Phi_{2p}(s_1)}, \ldots, \frac{\Phi_{2p}(q)}{\Phi_{2p}(s_k)}, \alpha_q^{(\pm)}\right).$$

Clearly, r and t are distinct, and r divides $\alpha_q^{(\pm)}$ and $|G:K|$ for all $K \in \mathcal{B}_t$. By Lemma 6, we conclude that r divides $P_G^{(t)}(0)$.

Finally, suppose that $\mathcal{S}_t = \varnothing$, i.e., $\mathcal{B}_t = \varnothing$. We leave it to the reader to check that $P_G^{(t)}(0) = 1 - q^p \alpha_q^{(\mp)}(q^{p-1} - 1)/(2p)$ is not a power of t. □

5. Irreducibility of the Dirichlet polynomial

Lemma 13 [Damian et al. 2004, Lemma 3]. *Let $n \in \mathbb{N}$. Then $1 - n/n^s$ is reducible in $\mathcal{R}$ if and only if n is a nontrivial power in $\mathbb{Z}$.*

Lemma 14. *Let $G = \mathrm{PSL}(2, q)$ with $f > 1$. Then $a_{q(q+1)/2}(G) \neq 0$.*

Proof. For $q \leq 25$ the result follows by direct inspection. For the remaining cases, note that every subgroup of G of order $2(q-1)/\delta$ is a maximal subgroup isomorphic to $D_{2(q-1)/\delta}$; see [Huppert 1967, p. 213]. □

Proposition 15. *Let G be as in the Main Theorem, with $f > 1$. Then $P_G(s)$ is irreducible in the ring of Dirichlet polynomials $\mathcal{R}$.*

Proof. Let $G = G(q, m)$, with $m \in \{1, 2, 3\}$. The proposition's validity when $m = 1$ and $q \in \{4, 8, 9\}$ is checked by direct inspection. For the rest of the proof, we exclude these three cases.

Suppose that $P_G(s) = g(s)h(s)$ for some Dirichlet polynomials $g(s)$ and $h(s)$ in $\mathcal{R}$. From (3-2) and case (1) in the proof of Proposition 12, we obtain

$$P_G^{(p)}(s) = 1 - \frac{p^{fm} + 1}{(p^{fm} + 1)^s}.$$

We claim that $P_G^{(p)}(s)$ is irreducible. We argue by contradiction. By Lemma 13, if $P_G^{(p)}(s)$ is reducible, then $p^{fm} + 1$ is a nontrivial power. Hence $p^{fm} + 1 = b^k$ for some $k \geq 2$ and $b \geq 1$, so there are no Zsigmondy primes for $\langle b, k\rangle$. By Lemma 4, (b, k) is either equal to $(2^{\omega} - 1, 2)$ for some $\omega \in \mathbb{N}$ or to $(2, 6)$. If $(b, k) = (2^{\omega} - 1, 2)$, then $p = 2$. Hence $fm = 3$, so $(q, m) = (8, 1)$, against assumption. Finally, if

$(b,k)=(2,6)$, then $p^{fm}+1=2^6$ has no solution. Therefore, without loss of generality, we suppose that $g^{(p)}(s)=1-(p^{fm}+1)/(p^{fm}+1)^s$ and $h^{(p)}(s)=1$.

Let t be a Zsigmondy prime for $\langle p, 2fm\rangle$. In particular, for $(m,f)=(1,2)$,

if 5^2 divides p^2+1, let $t=5$;
otherwise, let t be a Zsigmondy prime for $\langle p,4\rangle$ different from 5.

To see why this is possible, note that a Zsigmondy prime for $\langle p, 2fm\rangle$ exists since, by assumption, $2fm>2$ and $fm\neq 3$. If $(m,f)=(1,2)$, i.e., $(q,m)=(p^2,1)$, then, by assumption, p is odd. So $p^2+1=2a$ for some odd number a. Suppose that $5^2\nmid p^2+1$. Since we are assuming that $(q,m)\notin\{(4,1),(9,1)\}$, we conclude that p^2+1 does not divide 10. Hence there exists a Zsigmondy prime for $\langle p,4\rangle$ different from 5.

For a prime number r, let $\upsilon_r:\mathbb{Q}\to\mathbb{Z}\cup\{\infty\}$ be the r-adic valuation map. For a Dirichlet polynomial $f(s)\in\mathcal{R}$, define the integers $a_n(f)$, $n\in\mathbb{N}$, by the condition

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

Then $\max\{\upsilon_r(l):a_l(g)\neq 0\}+\max\{\upsilon_r(l):a_l(h)\neq 0\}=\max\{\upsilon_r(l):a_l(G)\neq 0\}$.

We claim that $h^{(t)}(s)=h(s)$. Indeed, since $a_{p^{fm}+1}(g)\neq 0$ and $\upsilon_t(p^{fm}+1)=\upsilon_t(|G|)$, we get

$$\max\{\upsilon_t(l):a_l(g)\neq 0\}=\max\{\upsilon_t(l):a_l(G)\neq 0\}.$$

So, if $a_l(h)\neq 0$, then t does not divide l. In particular, $h^{(t)}(s)=h(s)$, as claimed.

It follows that

$$P_G^{(t)}(s)=g^{(t)}(s)h(s). \tag{5-1}$$

Finally we show that $h(s)=1$.

Projective linear groups ($m=1$). Let r be an odd prime divisor of $q-1$ (recall that $q\neq 9$ and q is not a prime). Proposition 8, case (2), yields $P_G^{(t,r)}(s)=1$. Now (5-1) yields $h^{(r)}(s)=1$. So $P_G^{(r)}(s)$ is equal to $g^{(r)}(s)$. By Lemma 14, $a_{q(q+1)/2}(G)\neq 0$. Hence, since r does not divide $q(q+1)/2$, we get $a_{q(q+1)/2}(g(s))\neq 0$. It follows that

$$\max\{\upsilon_p(l):a_l(g)\neq 0\}=\max\{\upsilon_p(l):a_l(G)\neq 0\}.$$

Thus $h(s)=h^{(p)}(s)=1$.

Suzuki and Ree groups ($m=2,3$). In these cases, t clearly divides $\alpha_q^{(\pm)}$. Let r be a prime divisor of $\alpha_q^{(\mp)}$. By Proposition 12, case (4), we have $P_G^{(t,r)}(s)=1$. By (5-1), we get $h^{(r)}(s)=1$. Now $a_{p^{fm}+1}(g(s))\neq 0$ yields

$$\max\{\upsilon_r(l):a_l(g)\neq 0\}=\max\{\upsilon_r(l):a_l(G)\neq 0\}.$$

Hence $h(s) = h^{(r)}(s) = 1$. □

6. $P_G(-1)$ does not vanish

Proposition 16. *Let $G = G(q, m)$ be as in the Main Theorem. Then $P_G(-1) \neq 0$.*

Proof. Projective linear groups ($m = 1$). For $q \leq 11$ or $q = 49$, the proposition holds by direct inspection. Assume that q is greater than 11 and that $q \neq 49$.

Assume $f = 1$. By Proposition 8, case (1), we get

$$P_G(s) = 1 - \frac{p+1}{(p+1)^s} + \sum_{p \mid k} \frac{a_k(G)}{k^s}.$$

By Lemma 6, if p divides k, then p^2 divides $a_k(G)k$. Hence

$$P_G(-1) = 1 - (p+1)^2 + \sum_{p \mid k} a_k(G)k \equiv -2p \pmod{p^2}.$$

Assume $f \geq 2$. Let t be a Zsigmondy prime for $\langle p, 2f \rangle$. In particular, for $f = 2$,

if 5^3 divides $p^2 + 1$, let $t = 5$;
otherwise, let t be a Zsigmondy prime for $\langle p, 4 \rangle$ distinct from 5.

To see why this is possible, note that a Zsigmondy prime for $\langle p, 2f \rangle$ exists since $q \neq 8$ and $f \geq 2$. If $f = 2$, then, by assumption, p is odd. So $p^2 + 1 = 2a$ for some odd number a. Suppose that $5^3 \nmid p^2 + 1$. Since $q \notin \{4, 9, 49\}$ by assumption, $p^2 + 1$ does not divide 50. Hence there exists a Zsigmondy prime for $\langle p, 4 \rangle$ distinct from 5.

We observe that $t \neq 3$. As in the proof of Proposition 8, case (2), we obtain:

(a) $P_G(s) = 1 - \dfrac{q(q-1)/2}{[q(q-1)/2]^s} + \sum_{t \mid k} \dfrac{a_k(G)}{k^s}$.

(b) If M is a maximal subgroup of G, the index $|G : M|$ is divisible by t if and only if M is not isomorphic to $D_{2(q+1)/\delta}$. In particular, if M is not isomorphic to $D_{2(q+1)/\delta}$, we have $v_t(|G : M|) > v_t(|G|)/2$, where as before $v_t : \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$ is the t-adic valuation map.

(c) If M_1 and M_2 are distinct maximal subgroups isomorphic to $D_{2(q+1)/\delta}$, then $|G : M_1 \cap M_2|$ is divisible by $|G|/2$ or $M_1 \cap M_2$ is contained in a maximal subgroup not isomorphic to $D_{2(q+1)/\delta}$.

We claim that

$$P_G(-1) = -\frac{(q+1)(q-2)(q^2-q+2)}{4} + \sum_{t \mid k} k a_k(G) \not\equiv 0 \pmod{t^{v_t(|G|)+1}}.$$

In fact,

$$v_t\left(\frac{(q+1)(q-2)(q^2-q+2)}{4}\right) = v_t(q+1) = v_t(|G|).$$

Moreover, suppose that $a_k(G) \neq 0$ and that t divides k, for some $k > 1$. Then $v_t(k) > v_t(|G|)/2$. Indeed, by (b) and (c), the number k is divisible by $|G|/2$ or k divides the index of a maximal subgroup M such that t divides $|G:M|$ and $v_t(|G:M|) > v_t(|G|)/2$. Finally, by Lemma 6, we have $ka_k(G) \equiv 0 \pmod{t^{v_t(|G|)+1}}$.

Suzuki and Ree groups ($m = 2, 3$). Let t be a Zsigmondy prime for $\langle p, 2pf\rangle$. In particular, if $(p, f) = (2, 7)$, choose $t = 113$. Clearly $t \mid \alpha_q^{(\pm)}$.

We claim that if K is a subgroup of G and t divides $|G:K|$, then $v_t(|G:K|) = v_t(|G|)$. By Theorem 10 and 11, every maximal subgroup of G has this property. Moreover, if M is a maximal subgroup of G such that t does not divide $|G:M|$, then M is isomorphic to $B_\pm$. Finally, the index of the intersection of two distinct maximal subgroups isomorphic to $B_\pm$ is a multiple of $\alpha_q^{(\pm)}$; see the proof of Proposition 12, case (4).

Now, using Lemma 6, we get that if t divides k, then $t^{2v_t(|G|)}$ divides $ka_k(G)$. Again by case (4) in Proposition 12, we have

$$P_G(-1) = 1 - \left(\frac{q^p \alpha_q^{(\mp)}(q^{p-1}-1)}{2p}\right)^2 + \sum_{t\mid k} ka_k(G),$$

so $P_G(-1) \equiv 1 - \left(\frac{q^p \alpha_q^{(\mp)}(q^{p-1}-1)}{2p}\right)^2 \pmod{t^{2v_t(|G|)}}$. Finally

$$v_t\left(1 - \left(\frac{q^p \alpha_q^{(\mp)}(q^{p-1}-1)}{2p}\right)^2\right) = v_t(\alpha_q^{(\pm)}) = v_t(|G|).$$

Hence $P_G(-1) \neq 0$. □

7. Dirichlet polynomials of PSL(2, q), with $q = p^f$

We list here the Dirichlet polynomial $P(s) := P_{\mathrm{PSL}(2,q)}(s)$ for all values of q. We adopt the following conventions: μ is the usual Möbius function on positive integers; $r_h = \frac{1}{2}(p^h + 1)$; $v_h = \frac{1}{2}(p^h - 1)$; $r = r_f$; $v = v_f$; and $\alpha = 1$ if $f = 2^k$ for some $k > 1$, $\alpha = 0$ otherwise.

- For $q = 5$,

$$P(s) = 1 - \frac{5}{5^s} - \frac{6}{6^s} - \frac{10}{10^s} + \frac{20}{20^s} + \frac{60}{30^s} - \frac{60}{60^s}.$$

- For $q = 7$,

$$P(s) = 1 - \frac{14}{7^s} - \frac{8}{8^s} + \frac{21}{21^s} + \frac{28}{28^s} + \frac{56}{56^s} - \frac{84}{84^s}.$$

- For $q = 9$,

$$P(s) = 1 - \frac{12}{6^s} - \frac{10}{10^s} - \frac{30}{15^s} + \frac{60}{30^s} + \frac{36}{36^s} + \frac{45}{45^s} + \frac{240}{60^s} + \frac{90}{90^s} - \frac{240}{120^s} - \frac{900}{180^s} + \frac{720}{360^s}.$$

- For $q = 11$,

$$P(s) = 1 - \frac{22}{11^s} - \frac{12}{12^s} + \frac{66}{66^s} + \frac{220}{110^s} + \frac{132}{132^s} + \frac{165}{165^s} - \frac{220}{220^s} - \frac{990}{330^s} + \frac{660}{660^s}.$$

- For $q = p$, $p \equiv \pm 2 \pmod 5$, $p \equiv \pm 3 \pmod 8$,

$$P(s) = 1 - \frac{pv}{(pv)^s} - \frac{pr}{(pr)^s} - \frac{2r}{(2r)^s} + \frac{2pr}{(2pr)^s} - \frac{prv/6}{(prv/6)^s} + \frac{prv/2}{(prv/2)^s} + \frac{2prv/3}{(2prv/3)^s} + \frac{prv}{(prv)^s} - \frac{2prv}{(2prv)^s}.$$

- For $q = p$, $p \equiv \pm 2 \pmod 5$, $p \equiv \pm 1 \pmod 8$,

$$P(s) = 1 - \frac{pv}{(pv)^s} - \frac{pr}{(pr)^s} - \frac{2r}{(2r)^s} + \frac{2pr}{(2pr)^s} - \frac{prv/6}{(prv/12)^s} + \frac{prv/2}{(prv/4)^s} + \frac{2prv/3}{(prv/3)^s} - \frac{prv}{(prv)^s}.$$

- For $q = p$, $p \equiv \pm 1 \pmod 5$, $p \equiv \pm 3 \pmod 8$,

$$P(s) = 1 - \frac{pv}{(pv)^s} - \frac{pr}{(pr)^s} - \frac{2r}{(2r)^s} + \frac{2pr}{(2pr)^s} - \frac{prv/15}{(prv/30)^s} + \frac{prv/6}{(prv/6)^s} + \frac{2prv/5}{(prv/5)^s} + \frac{2prv/3}{(prv/3)^s} + \frac{prv/2}{(prv/2)^s} - \frac{2prv/3}{(2prv/3)^s} - \frac{3prv}{(prv)^s} + \frac{2prv}{(2prv)^s}.$$

- For $q = p$, $p \equiv \pm 1 \pmod 5$, $p \equiv \pm 1 \pmod 8$,

$$P(s) = 1 - \frac{pv}{(pv)^s} - \frac{pr}{(pr)^s} - \frac{2r}{(2r)^s} + \frac{2pr}{(2pr)^s} - \frac{prv/15}{(prv/30)^s} - \frac{prv/6}{(prv/12)^s} + \frac{prv/3}{(prv/6)^s} + \frac{2prv/5}{(prv/5)^s} + \frac{prv/2}{(prv/4)^s} + \frac{4prv/3}{(prv/3)^s} - \frac{4prv/3}{(2prv/3)^s} - \frac{5prv}{(prv)^s} + \frac{4prv}{(2prv)^s}.$$

- For $q = 2^f$, $f > 1$,

$$P(s) = \sum_{\substack{h \mid f \\ h > 1}} \mu\left(\frac{f}{h}\right)\left(\frac{2^{f-h}rv/(r_h v_h)}{[2^{f-h}rv/(r_h v_h)]^s} - \frac{2^{f-h+1}rv/v_h}{[2^{f-h+1}rv/v_h]^s} - \frac{2^f rv/v_h}{[2^f rv/v_h]^s} - \frac{2^f rv/r_h}{[2^f rv/r_h]^s} + \frac{2^{f+1}rv/r_h}{[2^{f+1}rv/r_h]^s}\right) + \mu(f)\left(-\frac{2^{f+2}rv}{[2^{f+1}rv]^s} + \frac{2^{f+2}rv}{[2^{f+2}rv]^s}\right).$$

- For $q = p^f$, $p \in \{3, 5\}$, $f > 1$ odd,

$$P(s) = \sum_{\substack{h \mid f \\ h > 1}} \mu(f/h)\left(\frac{p^{f-h}rv/(r_h v_h)}{[p^{f-h}rv/(r_h v_h)]^s} - \frac{2p^{f-h}rv/v_h}{[2p^{f-h}rv/v_h]^s} - \frac{p^f rv/v_h}{[p^f rv/v_h]^s} - \frac{p^f rv/r_h}{[p^f rv/r_h]^s} + \frac{2p^f rv/v_h}{[2p^f rv/v_h]^s}\right)$$
$$+\mu(f)\left(-\frac{p^{f-1}2rv}{[2p^{f-1}rv]^s} + \delta_{p,3}\left(\frac{3^f rv/6}{[3^f rv/6]^s} - \frac{3^f rv/2}{[3^f rv/2]^s} - \frac{3^f rv}{[3^f rv]^s} + \frac{2\cdot 3^f rv}{[2\cdot 3^f rv]^s}\right) + \delta_{p,5}\left(\frac{5^f rv/30}{[5^f rv/30]^s} - \frac{5^f rv/2}{[5^f rv/2]^s} - \frac{5^f rv/3}{[5^f rv/3]^s} + \frac{5^f rv}{[5^f rv]^s}\right)\right)$$

- For $q = p^f$, $p \geq 3$, $f \geq 4$ even or $p \equiv \pm 1, 0 \pmod 5$, $f = 2$

$$P(s) = \sum_{\substack{h|f \\ f/h \text{ odd}}} \mu(f/h)\biggl(\frac{p^{f-h}rv/(r_h v_h)}{[p^{f-h}rv/(r_h v_h)]^s} - \frac{2p^{f-h}rv/v_h}{[2p^{f-h}rv/v_h]^s} - \frac{p^f rv/v_h}{[p^f rv/v_h]^s} - \frac{p^f rv/r_h}{[p^f rv/r_h]^s} + \frac{2p^f rv/v_h}{[2p^f rv/v_h]^s}\biggr)$$
$$+ \sum_{\substack{h|f \\ f/h \text{ even}}} \mu(f/h)\biggl(\frac{p^{f-h}rv/(r_h v_h)}{[p^{f-h}rv/(2r_h v_h)]^s} - \frac{p^{f-h}2rv/v_h}{[p^{f-h}rv/v_h]^s} - \frac{p^f rv/v_h}{[p^f rv/(2v_h)]^s} - \frac{p^f rv/r_h}{[p^f rv/(2r_h)]^s} + \frac{2p^f rv/v_h}{[p^f rv/v_h]^s}\biggr) + \alpha\biggl(-\frac{p^f rv}{[p^f rv/2]^s} + \frac{p^f rv}{[p^f rv]^s}\biggr)$$

- For $q = p^2$, $p > 5$, $p \equiv \pm 2 \pmod 5$,

$$P(s) = 1 - \frac{2r}{(2r)^s} - \frac{p^2 r}{(p^2 r)^s} - \frac{p^2 v}{(p^2 v)^s} + \frac{2p^2 r}{(2p^2 r)^s} - \frac{2pr}{(pr)^s} + \frac{4prr_1}{(2prr_1)^s} + \frac{2p^2 rr_1}{(p^2 rr_1)^s}$$
$$+ \frac{2p^2 rv_1}{(p^2 rv_1)^s} - \frac{4p^2 rr_1}{(2p^2 rr_1)^s} - \frac{p^2 rv}{(p^2 rv/2)^s} - \frac{3p^2 rv}{(p^2 rv)^s} - \frac{p^2 rv/15}{(p^2 rv/30)^s}$$
$$+ \frac{p^2 rv/3}{(p^2 rv/6)^s} + \frac{2p^2 rv/5}{(p^2 rv/5)^s} + \frac{2p^2 rv/3}{(p^2 rv/3)^s} - \frac{4p^2 rv/3}{(2p^2 rv/3)^s} + \frac{4p^2 rv}{(2p^2 rv)^s}.$$

- For $q = p^f$, $p > 5$, $f > 1$ odd,

$$P(s) = \sum_{h|f} \mu(f/h)\biggl(\frac{p^{f-h}rv/(r_h v_h)}{[p^{f-h}rv/(r_h v_h)]^s} - \frac{2p^{f-h}rv/v_h}{[2p^{f-h}rv/v_h]^s} - \frac{p^f rv/v_h}{[p^f rv/v_h]^s} - \frac{p^f rv/r_h}{[p^f rv/r_h]^s} + \frac{2p^f rv/v_h}{[2p^f rv/v_h]^s}\biggr).$$

References

[Boston 1996] N. Boston, "A probabilistic generalization of the Riemann zeta function", pp. 155–162 in *Analytic number theory: proceedings of a conference in honor of Heini Halberstam* (Allerton Park, IL, 1995), vol. 1, edited by B. C. Berndt et al., Progr. Math. **138**, Birkhäuser, Boston, 1996. MR 97e:11106 Zbl 0853.11075

[Brown 2000] K. S. Brown, "The coset poset and probabilistic zeta function of a finite group", *J. Algebra* **225**:2 (2000), 989–1012. MR 2000k:20082 Zbl 0973.20016

[Damian and Lucchini 2003] E. Damian and A. Lucchini, "The Dirichlet polynomial of a finite group and the subgroups of prime power index", pp. 209–221 in *Advances in group theory 2002*, Aracne, Rome, 2003. MR 2005c:20036 Zbl 1070.20025

[Damian and Lucchini 2004] E. Damian and A. Lucchini, "Recognizing the alternating groups from their probabilistic zeta function", *Glasg. Math. J.* **46**:3 (2004), 595–599. MR 2005f:20113 Zbl 1071.20060

[Damian and Lucchini 2006] E. Damian and A. Lucchini, "On the Dirichlet polynomial of finite groups of Lie type", *Rend. Sem. Mat. Univ. Padova* **115** (2006), 51–69. MR 2008b:20017

[Damian and Lucchini 2007] E. Damian and A. Lucchini, "The probabilistic zeta function of finite simple groups", *J. Algebra* **313**:2 (2007), 957–971. MR 2008k:20041 Zbl 1127.20052

[Damian et al. 2004] E. Damian, A. Lucchini, and F. Morini, "Some properties of the probabilistic zeta function on finite simple groups", *Pacific J. Math.* **215**:1 (2004), 3–14. MR 2005b:20042 Zbl 1113.20063

[Detomi and Lucchini 2003a] E. Detomi and A. Lucchini, "Crowns and factorization of the probabilistic zeta function of a finite group", *J. Algebra* **265**:2 (2003), 651–668. MR 2004e:20119 Zbl 1072.20031

[Detomi and Lucchini 2003b] E. Detomi and A. Lucchini, "Recognizing soluble groups from their probabilistic zeta functions", *Bull. London Math. Soc.* **35**:5 (2003), 659–664. MR 2005a:20101 Zbl 1045.20054

[Downs 1991] M. Downs, "The Möbius function of $\mathrm{PSL}_2(q)$, with application to the maximal normal subgroups of the modular group", *J. London Math. Soc.* (2) **43**:1 (1991), 61–75. MR 92d:20071 Zbl 0743.20016

[Gaschütz 1959] W. Gaschütz, "Die Eulersche Funktion endlicher auflösbarer Gruppen", *Illinois J. Math.* **3** (1959), 469–476. MR 21 #6393 Zbl 0093.25002

[Hall 1936] P. Hall, "The Eulerian Functions of a group", *Quart. J. Math.* **7** (1936), 134–151. Zbl 0014.10402 JFM 62.0082.02

[Hawkes et al. 1989] T. Hawkes, I. M. Isaacs, and M. Özaydin, "On the Möbius function of a finite group", *Rocky Mountain J. Math.* **19**:4 (1989), 1003–1034. MR 90k:20046 Zbl 0708.20005

[Huppert 1967] B. Huppert, *Endliche Gruppen*, vol. I, Grundlehren der Math. Wiss. **134**, Springer, Berlin, 1967. MR 37 #302 Zbl 0217.07201

[Kleidman 1988] P. 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**:1 (1988), 30–71. MR 89j:20055 Zbl 0651.20020

[Mann 1996] A. Mann, "Positively finitely generated groups", *Forum Math.* **8**:4 (1996), 429–459. MR 97j:20029 Zbl 0852.20019

[Suzuki 1962] M. Suzuki, "On a class of doubly transitive groups", *Ann. of Math.* (2) **75** (1962), 105–145. MR 25 #112 Zbl 0106.24702

[Zsigmondy 1892] K. Zsigmondy, "Zur Theorie der Potenzreste", *Monatsh. Math. Phys.* **3**:1 (1892), 265–284. MR 1546236 Zbl 24.0176.02

Received February 26, 2008. Revised July 31, 2008.

MASSIMILIANO PATASSINI
UNIVERSITÀ DI PADOVA
DIPARTIMENTO DI MATEMATICA PURA ED APPLICATA
VIA TRIESTE, 63
PADOVA, 35121
ITALY

mpatassi@math.unipd.it