Bull. Austral. Math. Soc. Vol. 64 (2001) [121-129]

A THEOREM ON POWER SERIES WITH APPLICATIONS TO CLASSICAL GROUPS OVER FINITE FIELDS

ANDREW J. SPENCER

For some of the classical groups over finite fields it is possible to express the proportion of eigenvalue-free matrices in terms of generating functions. We prove a theorem on the monotonicity of the coefficients of powers of power series and apply this to the generating functions of the general linear, symplectic and orthogonal groups. This proves a conjecture on the monotonicity of the proportions of eigenvalue-free elements in these groups.

1. Introduction

In this paper we state and prove a result giving conditions for the coefficients of a power series raised to a power to decrease monotonically in size. This result has interesting consequences when used in conjunction with the results of Neumann and Praeger [1], on the proportion of eigenvalue-free matrices in the classical groups over finite fields.

We proceed as follows: Section 2 states and proves the main theorem of the paper; Section 3 introduces a function that was studied by Euler and states how this relates to the classical groups; Section 4 shows how we can use the techniques developed in Section 2 to work with the generating functions encountered in the previous section; Section 5 concludes with a result on the proportions of eigenvalue-free matrices in the general linear, symplectic and orthogonal groups over finite fields. Unless stated otherwise, all of our power series have real coefficients.

2. A THEOREM ON POWER SERIES

THEOREM 2.1. Suppose that $\lambda \in \mathbb{R}$ and $\lambda > 1$. Let $A(z) = \sum_{n=0}^{\infty} a_n z^n$, where $a_0 = 1$ and $0 < a_n \le a_{n-1}/\lambda$ for $n \ge 1$. If r is an integer such that $1 \le r \le \lambda$ and $a_n^{(r)}$ is the coefficient of z^n in $(A(z))^r$ then

$$0 < a_n^{(r)} < a_{n-1}^{(r)} \leqslant 1$$

for $n \ge 2$.

Received 30th October, 2000

Many thanks go to Dr Peter Neumann for his support and encouragement. I am also grateful to Duncan Brydon and the Engineering and Physical Sciences Research Council.

Copyright Clearance Centre, Inc. Serial-fee code: 0004-9727/01 \$A2.00+0.00.

We postpone the proof as it relies on the following lemma.

LEMMA 2.2. Let $R(z) = \sum_{n=0}^{\infty} r_n z^n$ and $S(z) = \sum_{n=0}^{\infty} s_n z^n$ where all $r_n, s_n > 0$ and the sequence $(r_n)_{n\geqslant 1}$ decreases strictly monotonically. Let T(z) = R(z)S(z) and write T(z) as $\sum_{n=0}^{\infty} t_n z^n$. For $n\geqslant 2$ if

$$r_0 s_n + r_1 s_{n-1} \leqslant r_0 s_{n-1}$$

then $t_n < t_{n-1}$.

PROOF: By definition,

$$t_n = r_0 s_n + r_1 s_{n-1} + \cdots + r_n s_0$$

and

$$t_{n-1} = r_0 s_{n-1} + r_1 s_{n-2} + \cdots + r_{n-1} s_0.$$

Since the coefficients of R(z) are strictly monotonically decreasing, for $2 \le i \le n$ we have $r_i s_{n-i} < r_{i-1} s_{n-i}$. The result follows.

PROOF OF THEOREM 2.1: Let $1 \leqslant r \leqslant \lambda$. We first deal with the coefficients $a_0^{(r)}$ and $a_1^{(r)}$. It is clear that $a_0^{(r)} = 1$ and we can show by induction that $a_1^{(r)} = ra_1$. As $a_1 \leqslant 1/\lambda$ and $1 \leqslant r \leqslant \lambda$ we see that $a_1^{(r)} \leqslant 1$. Note that $a_1^{(r)} = 1$ precisely when $r = \lambda$ and $a_1 = 1/\lambda$.

We shall now use induction on r, up to λ , to show that for $1 \leqslant r \leqslant \lambda$ and for all $n \geqslant 2$, the inequality $a_n^{(r)} < a_{n-1}^{(r)}$ holds. For r=1 we are just considering the power series A(z) for which the coefficients decrease strictly monotonically. Assume now that for some $r \leqslant \lambda - 1$ and for all $n \geqslant 2$ we have $a_n^{(r)} < a_{n-1}^{(r)}$. We apply Lemma 2.2 with $R(z) = (A(z))^r$ and S(z) = A(z). It follows that, for $n \geqslant 2$ if

(1)
$$a_0^{(r)}a_n + a_1^{(r)}a_{n-1} \leqslant a_0^{(r)}a_{n-1}$$

then

$$a_n^{(r+1)} < a_{n-1}^{(r+1)}$$
.

Therefore showing that (1) holds would complete the inductive step. Now $a_0^{(r)} = 1$ and $a_1^{(r)} = ra_1$. Furthermore, by assumption, $a_n \leq a_{n-1}/\lambda$, and $r \leq \lambda - 1$, so

$$a_0^{(r)}a_n + a_1^{(r)}a_{n-1} \leqslant \frac{1}{\lambda}a_{n-1} + ra_1a_{n-1} \leqslant a_{n-1}\left(\frac{1}{\lambda} + \frac{\lambda - 1}{\lambda}\right) = a_{n-1}a_0^{(r)},$$

as required.

3. Generating functions related to some classical groups over finite fields

We adopt the notation used by Neumann and Praeger in [1]. For a complex number x with |x| > 1 we define the function

$$G(x;z)=\prod_{i=1}^{\infty}(1-x^{-i}z).$$

It is shown in [1] that $G(x;z) = \sum_{n=0}^{\infty} a_n z^n$ where $a_0 = 1$ and for $n \ge 1$,

$$a_n = \frac{(-1)^n}{\prod_{i=1}^n (x^i - 1)}.$$

For $m \ge 1$, we shall be considering the classical groups GL(m,q), Sp(2m,q), $O^+(2m,q)$ and $O^-(2m,q)$ over the finite field \mathbb{F}_q . For $G \in \{GL, Sp, O^+, O^-\}$ we define v(G; m, q) to be the proportion of eigenvalue-free matrices in the corresponding group of appropriate dimension. When dealing with the orthogonal groups we define

$$v^{\pm}(O; m, q) = v(O^{+}; m, q) \pm v(O^{-}; m, q).$$

Considering these proportions as probabilities we define the associated generating functions

$$V(G; q, z) = 1 + \sum_{m=1}^{\infty} v(G; m, q) z^{m},$$

and

$$V^{\pm}(O; q, z) = 1 + \sum_{m=1}^{\infty} v^{\pm}(O; m, q) z^{m}.$$

It follows that

$$V(O^+; q, z) = \frac{1}{2} (V^+(O; q, z) + V^-(O; q, z))$$

and

$$V(\mathrm{O}^-;q,z) = \frac{1}{2} \left(V^+(\mathrm{O};q,z) - V^-(\mathrm{O};q,z) \right).$$

The results in Table 1 are proved in [1], expressing the generating functions in terms of the function G(x;z).

4. RESULTS ON THE GENERATING FUNCTIONS

For $G \in \{GL, Sp, O^+, O^-\}$ we now have expressions for V(G; q, z) in the form

$$V(G;q,z) = (1-z)^{-1} \sum_{n=0}^{\infty} a_n z^n.$$

Generating function	Related function
$V(\mathrm{GL};q,z)$	$(1-z)^{-1}G(q;z)^{q-1}$
$V(\mathrm{Sp};q,z)$	$(1-z)^{-1}G(q^2;qz)^2G(q;z)^{(q-3)/2}, q \text{ odd}$ $(1-z)^{-1}G(q^2;qz)G(q;z)^{(q-2)/2}, q \text{ even}$
$V^+(\mathrm{O};q,z)$	$(1-z)^{-1}G(q^2;qz)^2G(q;z)^{(q-3)/2}, q \text{ odd}$ $(1-z)^{-1}G(q^2;qz)G(q;z)^{(q-2)/2}, q \text{ even}$
$V^-(O;q,z)$	$G(q^2;z)^2G(q;z)^{(q-3)/2},\ q\ ext{odd} \ G(q^2;z)G(q;z)^{(q-2)/2},\ q\ ext{even}$

124

Table 1:

In this section we shall study these functions neglecting the factor $(1-z)^{-1}$ and prove results on the sequence $(a_n)_{n\geq 0}$. We say that the sequence $(a_n)_{n\geq n_0}$ is positive alternating if the sequence $((-1)^{n-n_0}a_n)_{n\geq n_0}$ has all terms greater than zero. We extend this definition to power series and define the class of positive alternating power series to be

$$C = \left\{ A(z) \mid A(z) = \sum_{n=0}^{\infty} (-1)^n a_n z^n, \ a_n > 0 \text{ for all } n \right\}.$$

It is not hard to show that \mathcal{C} is closed under multiplication. For $q \geq 2$ the functions G(q;z), $G(q^2;qz)$ and $G(q^2;z)$ all lie in \mathcal{C} and it follows that any product of these must also lie in \mathcal{C} . In particular, from Table 1, we see that $(1-z)V(\operatorname{GL};q,z)$, $(1-z)V(\operatorname{Sp};q,z)$, $(1-z)V^+(\operatorname{O};q,z)$ and $V^-(\operatorname{O};q,z)$ all lie in \mathcal{C} .

If we have a positive alternating power series $A(z) = \sum_{n=0}^{\infty} (-1)^n a_n z^n$ where all $a_n > 0$, then $A(-z) = \sum_{n=0}^{\infty} a_n z^n$. Hence to prove results on the monotonicity of the absolute value of the coefficients of A(z) we can work with the coefficients of A(-z) where all terms are positive.

THEOREM 4.1. Let $(1-z)V(GL;q,z) = \sum_{n=0}^{\infty} (-1)^n w_n z^n$. Then $w_0 = w_1$ and the sequence $(w_n)_{n \ge 1}$ is strictly monotonically decreasing.

PROOF: Consider the power series $G(q; -z)^{q-1}$. This is equal to $\sum_{n=0}^{\infty} w_n z^n$, where all $w_n > 0$. It is clear that $w_0 = 1$ and induction on the power of G(q; -z) gives $w_1 = 1$. If q = 2 then $G(q; -z)^{q-1} = G(2; -z)$. In this case $(w_n)_{n \geqslant 1}$ is strictly monotonically decreasing and so we may assume that $q \geqslant 3$. Let a_n be the coefficient of z^n in G(q; -z). We know that for all $n \geqslant 1$,

$$a_n = \frac{a_{n-1}}{q^n - 1} \leqslant \frac{a_{n-1}}{q - 1},$$

and so we apply Theorem 2.1 to G(q; -z) with $\lambda = q - 1$. This gives $w_n < w_{n-1}$ for all $n \ge 2$, as required.

THEOREM 4.2. Let $(1-z)V(\operatorname{Sp};q,z)=\sum_{n=0}^{\infty}(-1)^nw_nz^n$. Then the sequence $(w_n)_{n\geq 0}$ is strictly monotonically decreasing.

PROOF: We just prove the case when $q \ge 3$ and q is odd. A similar argument works for even q. We know that

$$(1-z)V(\operatorname{Sp};q,z) = G(q^2;qz)^2G(q;z)^{(q-3)/2}$$

We shall work with the function

$$G(q^2; -qz)^2 G(q; -z)^{(q-3)/2}$$

which has coefficients $(w_n)_{n\geq 0}$ that are all positive. We first show that the coefficients of $G(q^2; -qz)G(q; -z)^{(q-3)/2}$ decrease strictly monotonically. If q=3 this is clear and we consider $q\geq 5$. Let

$$A(z) = G(q; -z)^{(q-3)/2} = \sum_{n=0}^{\infty} a_n z^n, \quad B(z) = G(q^2; -qz) = \sum_{n=0}^{\infty} b_n z^n.$$

From Theorem 2.1 we know that the terms of the sequence $(a_n)_{n\geqslant 0}$ decrease strictly monotonically. We can use this together with Lemma 2.2 to see that A(z)B(z) has coefficients which decrease strictly monotonically if, for $n\geqslant 1$, $a_0b_n+a_1b_{n-1}< a_0b_{n-1}$. Induction gives that

$$a_1 = \frac{q-3}{2(q-1)}$$

and we know that

$$b_n = b_{n-1} \frac{q}{q^{2n} - 1}.$$

Therefore we need to show that

$$\frac{q}{q^{2n}-1}+\frac{q-3}{2(q-1)}<1.$$

This certainly holds for $n \ge 1$ and $q \ge 5$. Having proved that the coefficients of $G(q^2; -qz)G(q; -z)^{(q-3)/2}$ are strictly monotonically decreasing we repeat the technique. This time let $A(z) = G(q^2; -qz)G(q; -z)^{(q-3)/2}$ and $B(z) = G(q^2; -qz)$, again with coefficients $(a_n)_{n\ge 0}$ and $(b_n)_{n\ge 0}$. Calculations give that $a_0 = 1$ and

$$a_1 = \frac{q}{q^2 - 1} + \frac{q - 3}{2(q - 1)}.$$

Therefore to prove that A(z)B(z) has coefficients that decrease strictly monotonically we must show that for $n \ge 1$, $a_0b_n + a_1b_{n-1} < a_0b_{n-1}$, that is,

$$\frac{q}{q^{2n}-1}+\frac{q}{q^2-1}+\frac{q-3}{2(q-1)}<1.$$

This can be seen to hold for all $q \ge 3$ and $n \ge 1$. The coefficients of A(z)B(z) are precisely the sequence $(w_n)_{n\ge 0}$, and so the proof is complete.

THEOREM 4.3. Let $(1-z)V(O^+;q,z) = \sum_{n=0}^{\infty} w_n z^n$. Then the sequence $(w_n)_{n\geqslant 0}$ is positive alternating, $w_0 = |w_1| = 1$ and $(|w_n|)_{n\geqslant 1}$ decreases strictly monotonically. We omit the proof as it is similar to that of the next theorem.

THEOREM 4.4. Let $(1-z)V(O^-;q,z) = \sum_{n=0}^{\infty} w_n z^n$. Then the sequence $(w_n)_{n\geqslant 1}$ is positive alternating, $w_0 = 0$ and $(|w_n|)_{n\geqslant 1}$ decreases strictly monotonically. Before we prove this we obtain some information about the power series $G(q^2;z)^2$.

LEMMA 4.5. Let a_n be the coefficient of z^n in the power series $G(q^2; z)^2$. For $q \ge 3$ and $n \ge 1$ we have

$$|a_{n-1}| > q^n |a_n|.$$

PROOF: Let us denote the coefficient of z^n in the power series $G(q^2; -z)$ by c_n . It follows that

$$|a_n| = \sum_{i=0}^n c_i c_{n-i}.$$

Suppose that n is odd and $n \ge 3$. Here we have

$$|a_n| = 2c_0c_n + 2c_1c_{n-1} + \dots + 2c_{(n-1)/2}c_{(n+1)/2},$$

$$|a_{n-1}| = 2c_0c_{n-1} + 2c_1c_{n-2} + \dots + 2c_{(n-3)/2}c_{(n+1)/2} + c_{(n-1)/2}c_{(n-1)/2}.$$

We compare these equations term by term and claim that for $n \ge 3$ and $1 \le i \le (n+1)/2$ we have $c_{n-i} > 2q^n c_{n-i+1}$. To prove this claim we note that

$$c_{n-i+1} = \frac{c_{n-i}}{q^{2(n-i+1)} - 1}$$

and so

$$c_{n-i} - 2q^n c_{n-i+1} = \left(1 - \frac{2q^n}{q^{2(n-i+1)} - 1}\right) c_{n-i}.$$

Now $c_{n-i} > 0$ and for i and n in the range above,

$$\frac{2q^n}{q^{2(n-i+1)}-1}<1.$$

Hence $c_{n-i} - 2q^n c_{n-i+1} > 0$ as required. The case when n is even is similar and checking that $|a_0| > q|a_1|$ completes the proof.

PROOF OF THEOREM 4.4: Suppose first that q is even and $q \ge 2$. In this case

$$V(\mathcal{O}^-;q,z) = \frac{1}{2}(1-z)^{-1}G(q;z)^{(q-2)/2}\left(G(q^2;qz) - (1-z)G(q^2;z)\right).$$

Let $H(q;z) = G(q^2;qz) - (1-z)G(q^2;z)$ with coefficients $(h_n)_{n\geq 0}$. It is not difficult to show that $h_0 = 0$ and for $n \geq 1$,

$$h_n = (-1)^{n-1} \frac{q^n(q^n - 1)}{\prod_{i=1}^n (q^{2i} - 1)}.$$

Clearly $(h_n)_{n\geq 1}$ is positive alternating and for $n\geq 2$,

$$\frac{|h_n|}{|h_{n-1}|} = \frac{q}{(q^n+1)(q^{n-1}-1)} < 1,$$

telling us that the sequence $(|h_n|)_{n\geq 1}$ is strictly monotonically decreasing. Writing

$$(1-z)V(O^-;q,z) = \frac{1}{2}G(q;z)^{(q-2)/2}H(q;z)$$

as $\sum_{n=0}^{\infty} w_n z^n$ we see that $w_0 = 0$ and $(w_n)_{n\geqslant 1}$ is positive alternating. If q=2 then $(1-z)V(O^-;q,z) = H(q;z)/2$, the coefficients of which satisfy the required monotonicity conditions. We may therefore assume that $q\geqslant 4$. We know from Theorem 2.1 that $G(q;-z)^{(q-2)/2}$ has coefficients that decrease strictly monotonically. With a little work we can apply Lemma 2.2 to $G(q;-z)^{(q-2)/2}$ and -H(q;-z) to see that the sequence $(|w_n|)_{n\geqslant 1}$ decreases strictly monotonically.

Suppose now that $q \ge 3$ and q is odd. Here

$$V(\mathrm{O}^-;q,z) = \frac{1}{2}(1-z)^{-1}G(q;z)^{(q-3)/2}\left(G(q^2;qz)^2 - (1-z)G(q^2;z)^2\right).$$

Let $H(q;z) = G(q^2;qz)^2 - (1-z)G(q^2;z)^2$ with coefficients $(h_n)_{n\geqslant 0}$ and let a_n be the coefficient of z^n in $G(q^2;z)^2$. It is clear that $h_0 = 0$ and for $n \geqslant 1$,

$$h_n = q^n a_n - a_n + a_{n-1}.$$

We know that the sequence $(a_n)_{n\geqslant 0}$ is positive alternating and for all $n\geqslant 1$, Lemma 4.5 tells us that $|a_{n-1}|>q^n|a_n|$. Therefore h_n has the same sign as a_{n-1} and

(2)
$$|h_n| = |a_{n-1}| - (q^n - 1)|a_n|.$$

If $n \ge 2$, Equation 2 gives

$$|h_{n-1}| - |h_n| = |a_{n-2}| - q^{n-1}|a_{n-1}| + (q^n - 1)|a_n|.$$

It is clear that $(q^n-1)|a_n|>0$ and Lemma 4.5 tells us that $|a_{n-2}|>q^{n-1}|a_{n-1}|$. Hence for all $n\geqslant 2$, $|h_n|<|h_{n-1}|$ and so $(|h_n|)_{n\geqslant 1}$ is strictly monotonically decreasing. This proves the theorem in the case q=3 as here $(1-z)V(O^-;q,z)=H(q;z)/2$. Assuming that $q\geqslant 5$, we consider the power series $G(q;z)^{(q-3)/2}H(q;z)$. Since $h_0=0$, it is clear

that the first coefficient in this power series is equal to zero, and after this the coefficients are positive alternating. Let us define

$$F(z) = -H(q; -z), \quad E(z) = G(q; -z) = \sum_{n=0}^{\infty} e_n z^n.$$

We shall work with $E(z)^{(q-3)/2}F(z)$ as, neglecting sign, it has the same coefficients as $G(q;z)^{(q-3)/2}H(q;z)$, that is $2(1-z)V(O^-;q,z)$. Therefore, it remains to prove that $E(z)^{(q-3)/2}F(z)$ has coefficients that, after the first, decrease strictly monotonically in size. For $0 \le k \le (q-3)/2$ we define

$$S^{(k)}(z) = E(z)^k F(z)$$

and we denote its coefficients by $(s_n^{(k)})_{n\geq 0}$. For $k\geq 0$ we see that

$$s_0^{(k)} = 0$$
, $s_1^{(k)} = \frac{q-1}{q+1}$ and $s_2^{(k)} = \frac{1}{q^2+1} + \frac{k}{q+1}$.

We want to use induction on k up to (q-3)/2 to prove that the sequence $(s_n^{(k)})_{n\geqslant 1}$ is strictly monotonically decreasing. By definition $S^{(0)}(z)=F(z)=-H(q;-z)$ which we have already studied. Suppose that for some k, $0\leqslant k\leqslant (q-5)/2$, the sequence $(s_n^{(k)})_{n\geqslant 1}$ is strictly monotonically decreasing. We want to prove the condition for $S^{(k+1)}(z)$. An argument similar to that in the proof of Lemma 2.2 shows that for $n\geqslant 2$, if

(3)
$$s_0^{(k)} e_n + s_1^{(k)} e_{n-1} + s_2^{(k)} e_{n-2} < s_0^{(k)} e_{n-1} + s_1^{(k)} e_{n-2}$$

then $s_n^{(k+1)} < s_{n-1}^{(k+1)}$. Observing that $e_{n-1} = e_{n-2}/(q^{n-1}-1)$ and substituting the values of $s_0^{(k)}$, $s_1^{(k)}$, and $s_2^{(k)}$ we see that Equation 3 holds for n and k in the ranges specified. This completes the induction and the proof.

It is worth noting that we can find values of q for which the coefficients of the power series (1-z)V(U;q,z), associated with the unitary groups U(m,q), are neither alternating in sign nor monotonically decreasing in absolute value. In [1, p.579], there are a couple of mistakes. Firstly $G(-q;-z)^{q+1}G(q^2;z)^{-(q^2-q-2)/2}$ is written in two places instead of $G(-q;-z)^{q+1}G(q^2;z)^{(q^2-q-2)/2}$. Secondly the assertion is made that the coefficients of (1-z)V(U;q,z) alternate in sign for $q \ge 4$. As stated above, this is false.

5. CONCLUDING REMARKS

From the fact that the generating function $V^-(O;q,z)\in\mathcal{C}$, we deduce that for even m

$$v(O^+; m, q) > v(O^-; m, q)$$

and for odd m

$$v(O^+; m, q) < v(O^-; m, q).$$

Suppose that we fix a prime power q and $G \in \{GL, Sp, O^+, O^-\}$. For $m \ge 1$ we define $v_m = v(G; m, q)$. It is proved in [1] that these probabilities all tend to limits as $m \to \infty$ and we write $v_\infty = \lim_{m \to \infty} v_m$.

THEOREM 5.1. If $G \in \{GL, Sp, O^+\}$ then

$$v_{2m-1} < v_{2m+1} < v_{\infty} < v_{2m+2} < v_{2m}$$
.

If $G = O^-$ then

$$v_{2m-1} > v_{2m+1} > v_{\infty} > v_{2m+2} > v_{2m}$$
.

PROOF: Suppose that we write the generating function V(G;q,z) in the form

(4)
$$V(G;q,z) = (1-z)^{-1} \sum_{n=0}^{\infty} w_n z^n,$$

then for all $m \geqslant 1$,

$$v_m = \sum_{i=0}^m w_i.$$

Furthermore, if the sequence $(w_n)_{n\geqslant 0}$ is positive alternating, the terms of $(w_n)_{n\geqslant 1}$ decrease strictly monotonically in absolute value, and the series $\sum w_n$ converges, then

$$v_{2m-1} < v_{2m+1} < v_{\infty} < v_{2m+2} < v_{2m}$$

This is the situation when $G \in \{GL, Sp, O^+\}$. When $G = O^-$ the inequalities are reversed since expressing $V(O^-; q, z)$ in the form (4) yields a sequence $(w_n)_{n\geqslant 0}$ that is positive alternating and whose terms decrease strictly monotonically in absolute value only after the first term $(w_0 = 0)$ has been removed.

It would be interesting to see a combinatorial explanation for these inequalities.

REFERENCES

[1] P.M. Neumann and C.E. Praeger, 'Derangements and eigenvalue-free elements in finite classical groups', J. London Math. Soc. (2) 58 (1998), 564-586.

St. Hugh's College Oxford OX2 6LE United Kingdom