

COUNTING CYCLIC AND SEPARABLE MATRICES OVER A FINITE FIELD

G.E. WALL

To Bernhard Neumann on his ninetieth birthday

Australiam fato profugus Griffinaque venit litora, ...

A square matrix is called cyclic if its characteristic and minimum polynomials coincide, separable if the characteristic polynomial has no repeated roots. Recent results of P. Neumann and Praeger, and of Lehrer, about the numbers of such matrices over a finite field are sharpened.

1. INTRODUCTION

Let $M = M(n, q)$ denote the algebra of all $n \times n$ matrices over the finite field \mathbb{F}_q (q a prime-power) and $G = GL(n, q)$ the corresponding general linear group. By standard matrix theory, the characteristic and minimum polynomials, $c_X(t)$ and $m_X(t)$, of an element X of M satisfy the relations

$$d_X(t) \mid m_X(t) \mid c_X(t),$$

where $d_X(t)$ denotes the product of the distinct irreducible factors of $c_X(t)$. We call X cyclic if $c_X(t) = m_X(t)$, separable if $c_X(t) = d_X(t)$. These are the regular and regular semisimple elements of M in the sense of the theory of algebraic groups.

Denote by $c_M(n, q), c_G(n, q)$ the proportions of cyclic elements in M, G respectively and by $s_M(n, q), s_G(n, q)$ the corresponding proportions of separable elements. Several results about these ratios have been proved in two recent papers. P. Neumann and Praeger [3], with applications to computational algorithms in mind, obtain numerical bounds for $c_M(n, q)$ and $s_M(n, q)$. Lehrer [1], in the course of an investigation into the variety of regular semisimple elements in an algebraic group, derives explicit formulae for $s_M(n, q), s_G(n, q)$ and proves a “stability” result about their expansions in powers of q^{-1} . Here we shall prove somewhat sharper versions of these results. For generalisations to other algebraic groups, which are not touched on here, see Lehrer [1] and forthcoming papers by Neumann, Praeger and J.E. Fulman.

Received 12th May, 1999

Copyright Clearance Centre, Inc. Serial-fee code: 0004-9727/99 \$A2.00+0.00.

Two of the main results of [3] are that, for $n \geq 2$,

$$(1.1) \quad \frac{1}{q^2(q+1)} < 1 - c_M(n, q) < \frac{1}{(q^2-1)(q-1)},$$

$$(1.2) \quad q^{-1} + q^{-2} + q^{-3} < 1 - s_M(n, q) < \frac{q^2}{(q^2-1)(q-1)} + \frac{1}{2}q^{-2} + \frac{2}{3}q^{-3}.$$

Thus, for every $n \geq 2$, the proportions of *noncyclic* and *nonseparable* elements in $M(n, q)$ are, to a first approximation, q^{-3} and q^{-1} respectively. While these inequalities accurately focus on the numerical values of $c_M(n, q)$ and $s_M(n, q)$ for large q , they are less effective for small q . For example, when $q = 2$ the bounds in (1.1) are $1/12$ and $1/3$.

It is shown here that the four ratios $c_M(n, q), \dots$ tend to limits $c_M(\infty, q), \dots$ as $n \rightarrow \infty$. These limits are evaluated explicitly and estimates are given of the rates at which they are approached. Our results for the c ratios improve on those of Neumann and Praeger and provide good estimates for small q . The results for the s ratios are less satisfactory: our bounds, although of the right order of magnitude asymptotically, give poor results for small n and q .

It is easily seen that all four ratios can be expanded as power series in q^{-1} with rational coefficients. It is therefore natural to expect that they have the same limiting values in the sense of the formal power series norm $\|\cdot\|_q$ given by

$$(1.3) \quad \left\| \sum a_n q^{-n} \right\|_q = q^{-m},$$

where m is the least n for which $a_n \neq 0$. We show that this is indeed the case and get detailed information about the rate of convergence in the sense of the new norm. Lehrer [1] derives an explicit formula for $s_M(n, q)$ (his $K_n(q)$) and shows (Proposition 8.6) that

$$(1.4) \quad \|s_M(n, q) - s_M(\infty, q)\|_q \leq q^{-1 - [n/2]},$$

where $[r]$ denotes the integral part of r . We show that

$$(1.5) \quad \|s_M(n, q) - s_M(\infty, q)\|_q \leq q^{-n}$$

with equality if, and only if, $n - 1$ is a triangular number:

$$(1.6) \quad n - 1 = \frac{1}{2}m(m + 1) \quad (m = 0, 1, 2, \dots).$$

As a by-product of these results, we verify Lehrer's conjecture (in Example 8.8) that every coefficient in the expansion of $s_M(\infty, q)$ is 0, 1 or -1 .

We end this Introduction with a brief section by section survey of the paper. Of central importance are two closely related generating functions

$$(1.7) \quad P(q, t) = \sum_{n=0}^{\infty} a(n, q)t^n ,$$

$$(1.8) \quad P^+(q, t) = \sum_{n=0}^{\infty} a^+(n, q)t^n .$$

These are defined, and their relations to the four ratios explained, in Section 2. The simple expressions for $c_M(n, q), c_G(n, q)$ in terms of the coefficients in (1.7), (1.8) suffice, in Section 3, to prove the existence of the limits $c_M(\infty, q), c_G(\infty, q)$ and to get quite good estimates of the rates at which they are approached. The object of Section 4 is to show that

$$(1.9) \quad a(n, q) = A_n(q^{-1}), \quad a^+(n, q) = A_n^+(q^{-1}) ,$$

where $A_n(t), A_n^+(t)$ are rational functions with rational coefficients. Since all the poles of these rational functions are roots of unity, it follows that $a(n, q), a^+(n, q)$ can be expanded as power series in q^{-1} .

Replacing the indeterminate t by a complex variable z , we get a function $P(q, z)$ analytic for $|z| < 1$. The main result of Section 5 is that $P(q, z) - 1/(1 - z)$ is analytic for $|z| < q$, implying that

$$(1.10) \quad \lim_{n \rightarrow \infty} (a(n, q) - 1)r^n = 0$$

whenever $0 \leq r < q$, and a fortiori that

$$(1.11) \quad \lim_{n \rightarrow \infty} a(n, q) = 1 .$$

The limit (1.11) is the key to the explicit evaluation of the four limits $c_M(\infty, q), \dots$ in Section 6. A modified version of (1.10) is used in the same section to estimate the rates of convergence for the s ratios.

We turn in Section 7 to limits in the sense of the norm $\|\cdot\|_q$, and here the considerations are again purely formal. By carefully examining $\log((1 - t)P(q, t))$, we show that

$$(1.12) \quad P(q, t) - \frac{1}{1 - t} = B(1/q, t/q)$$

with a certain 2-variable formal power series $B(u, t)$. This result in fact implies (1.5), the condition for equality following from the subsidiary result that

$$(1.13) \quad B(0, t) = \sum_{m=0}^{\infty} t^{1+m(m+1)/2} .$$

It would be interesting to know the precise domain of holomorphy of the function $B(w, z)$ of two complex variables w, z : it appears to contain the region $|w| + |z| < 1$.

The results of this paper could be substantially improved if more were known about the coefficient of the powers of t in the numerators of the rational functions $A_n(t), A_n^+(t)$. As briefly mentioned at the end of Section 4, Lehrer [1] has given a very interesting interpretation of the formulae for these coefficients as sums of inner products of certain generalised characters of the symmetric group S_n . Further relevant information is given in the recent paper of Lehrer and Segal [2].

2. GENERATING FUNCTIONS

In this section we shall derive infinite product formulae for generating functions $C_M(q, t), \dots$ associated with the four ratios $c_M(n, q), \dots$. By convention, these ratios have the value 1 when $n = 0$.

It is convenient to begin with

$$(2.1) \quad C_G(q, t) = \sum_{n=0}^{\infty} c_G(n, q)t^n .$$

Let Γ denote the set of all cyclic elements of $G = GL(n, q)$ and consider the conjugation action of G on Γ . By standard matrix theory, two elements of Γ lie in the same orbit if, and only if, they have the same characteristic polynomial: let Γ_f denote the orbit formed by the elements of Γ with characteristic polynomial $f = f(t)$. If $X \in \Gamma_f$, the elements of $M = M(n, q)$ that commute with it form a subalgebra isomorphic to

$$R_f = \mathbb{F}_q[t]/f(t)\mathbb{F}_q[t] ,$$

and its stabiliser in G is isomorphic to the group of units, R_f^* , of R_f . Hence

$$|\Gamma_f| = |G| / |R_f^*| .$$

It follows that

$$(2.2) \quad c_G(n, q) = \sum_f^+ |R_f^*|^{-1} ,$$

where summation \sum^+ is over the monic $f(t)$ of degree n in $\mathbb{F}_q[t]$ such that $f(0) \neq 0$.

We observe now that, if $f(t), g(t)$ are relatively prime, then

$$R_{fg} \cong R_f \oplus R_g$$

and so

$$R_{fg}^* \cong R_f^* \times R_g^* .$$

It follows that

$$|R_f^*| = \prod |R_{p^\lambda}^*| ,$$

where $f = \prod p^\lambda$ is the prime factor decomposition.

If $p = p(t)$ is a monic irreducible polynomial of degree d , write

$$F_p(t) = 1 + \sum_{\lambda=1}^{\infty} t^{d\lambda} / |R_{p^\lambda}^*| .$$

Then the above considerations show that

$$C_G(q, t) = \prod^+ F_p(t) ,$$

where the product \prod^+ is taken over all monic irreducible polynomials $p(t)$ except t .

Now, $F_p(t)$ depends only on q and the degree d of $p(t)$. For R_{p^λ} is a local ring of order $q^{d\lambda}$ whose maximal ideal has order $q^{d(\lambda-1)}$, so that

$$|R_{p^\lambda}^*| = q^{d\lambda} - q^{d(\lambda-1)} .$$

Therefore

$$\begin{aligned} F_p(t) &= 1 + \sum_{\lambda=1}^{\infty} t^{d\lambda} / (q^{d\lambda} - q^{d(\lambda-1)}) \\ &= \left[(1 - u^d)^{-1} \left(1 + u^d / (q^d - 1) \right) \right]_{u=t/q} \end{aligned}$$

Define $N^+(d, q)$ by

$$(2.3) \quad \left. \begin{aligned} N^+(1, q) &= N(1, q) - 1 , \\ N^+(d, q) &= N(d, q) (d \geq 2) , \end{aligned} \right\}$$

where $N(d, q)$ is the number of monic irreducible polynomials of degree d in $\mathbb{F}_q[t]$. Putting together the results above, we conclude that

$$C_G(q, t) = [L^+(q, u)P^+(q, u)]_{u=t/q} ,$$

where

$$(2.4) \quad \begin{aligned} L^+(q, u) &= \prod_{d=1}^{\infty} (1 - u^d)^{-N^+(d, q)} , \\ P^+(q, u) &= \prod_{d=1}^{\infty} (1 + u^d / (q^d - 1))^{N^+(d, q)} . \end{aligned}$$

The formula for $C_G(q, t)$ can be simplified a little further. By its form, $L^+(q, u)$ is the generating function for the number of monic polynomials $f(t)$ in $\mathbb{F}_p[t]$ of given degree such that $f(0) \neq 0$. In other words,

$$\begin{aligned} L^+(q, u) &= 1 + \sum_{\lambda=1}^{\infty} q^{\lambda-1}(q-1)u^\lambda \\ &= (1-u)(1-qu)^{-1} . \end{aligned}$$

Thus we have finally

$$(2.5) \quad (1-t)C_G(q, t) = [(1-u)P^+(q, u)]_{u=t/q} .$$

The explicit values of $N(n, q)$ and $N^+(n, q)$ are well known : by counting the elements, and the nonzero elements, of \mathbb{F}_{q^n} in two different ways, one gets the summation formulae

$$(2.6) \quad \sum_{d|n} dN(d, q) = q^n \quad (n \geq 1) ,$$

$$(2.7) \quad \sum_{d|n} dN^+(d, q) = q^n - 1 \quad (n \geq 1) ,$$

whence, by the Möbius inversion formula,

$$(2.8) \quad N(n, q) = \frac{1}{n} \sum_{d|n} \mu(n/d)q^d ,$$

$$(2.9) \quad N^+(n, q) = \frac{1}{n} \sum_{d|n} \mu(n/d)(q^d - 1) .$$

The calculation of

$$(2.10) \quad S_G(q, t) = \sum_{n=0}^{\infty} s_G(n, q)t^n$$

follows the same lines, except that only polynomials f with no repeated irreducible factors are to be taken into account. Thus, $F_p(t)$ is replaced by

$$1 + t^d/|R_p^*| = 1 + t^d/(q^d - 1)$$

and we find that

$$(2.11) \quad S_G(q, t) = P^+(q, t) .$$

The formulae for $c_M(n, q)$ and $s_M(n, q)$ corresponding to (2.2) involve the extra factor

$$(2.12) \quad \omega(n, q) = \frac{|GL(n, q)|}{|M(n, q)|} = \prod_{i=1}^n (1 - q^{-i}).$$

For example, we have

$$c_M(n, q) = \omega(n, q) \sum_f |R_f^*|^{-1},$$

where summation \sum is now over *all* monic f of degree n . Accordingly, we introduce the modified generating function

$$(2.13) \quad C_M(q, t) = \sum_{n=0}^{\infty} (c_M(n, q)/\omega(n, q)) t^n.$$

The previous arguments now carry through to give

$$C_M(q, t) = [L(q, u)P(q, u)]_{u=t/q},$$

where

$$(2.14) \quad \begin{aligned} L(q, u) &= \prod_{d=1}^{\infty} (1 - u^d)^{-N(d, q)}, \\ P(q, u) &= \prod_{d=1}^{\infty} (1 + u^d/(q^d - 1))^{N(d, q)} \end{aligned}$$

The form of $L(q, u)$ identifies it as the generating function for the number of monic polynomials of given degree, so that

$$L(q, u) = 1 + \sum_{\lambda=1}^{\infty} q^\lambda u^\lambda = (1 - qu)^{-1}.$$

Hence finally

$$(2.15) \quad (1 - t) C_M(q, t) = [P(q, u)]_{u=t/q}.$$

For the modified generating function

$$(2.16) \quad S_M(q, t) = \sum_{n=0}^{\infty} (s_M(n, q)/\omega(m, q)) t^n,$$

we find in the same way that

$$(2.17) \quad S_M(q, t) = P(q, t) .$$

The following identities, implicit in the results above, are set down for reference:

$$(2.18) \quad P(q, u) = (1 + u/(q - 1))P^+(q, u) ,$$

$$(2.19) \quad (1 - qu) = \prod_{d=1}^{\infty} (1 - u^d)^{N(d,q)} .$$

Up to degree 4, we have

$$(2.20) \quad P(q, u) = 1 + \left(1 + \frac{1}{q-1}\right)u + \left(1 + \frac{1}{q^2-1}\right)u^2 + \left(1 - \frac{1}{(q^2-1)(q^3-1)}\right)u^3 + \left(1 + \frac{q^5+1}{(q^2-1)(q^3-1)(q^4-1)}\right)u^4 + \dots ,$$

$$(2.21) \quad P^+(q, u) = 1 + u + \left(1 - \frac{1}{q} - \frac{1}{q(q^2-1)}\right)u^2 + \left(1 - \frac{1}{q} + \frac{q^2+1}{q(q^2-1)(q^3-1)}\right)u^3 + \left(1 - \frac{1}{q} + \frac{q^5-2q^4+q^3-3q^2+q-1}{q(q-1)(q^3-1)(q^4-1)}\right)u^4 \dots .$$

3. IMMEDIATE ESTIMATES

Let

$$(3.1) \quad P(q, u) = \sum_{n=0}^{\infty} a(n, q)u^n ,$$

$$(3.2) \quad P^+(q, u) = \sum_{n=0}^{\infty} a^+(n, q)u^n .$$

By (2.18),

$$(3.3) \quad a(n, q) = a^+(n, q) + a^+(n - 1, q)/(q - 1) .$$

It is evident that $a(n, q), a^+(n, q)$ are rational functions of q with rational coefficients. Their form will be examined in greater detail in Section 4.

The expressions for the generating functions $C_M(q, t), \dots$ in terms of $P(q, u), P^+(q, u)$ derived in Section 2 translate into the following relations between their coefficients:

$$(3.4) \quad c_M(n, q)/\omega(n, q) - c_M(n - 1, q)/\omega(n - 1, q) = a(n, q)q^{-n} ,$$

$$(3.5) \quad c_G(n, q) - c_G(n - 1, q) = (a^+(n, q) - a^+(n - 1, q))q^{-n} ,$$

$$(3.6) \quad s_M(n, q)/\omega(n, q) = a(n, q) ,$$

$$(3.7) \quad s_G(n, q) = a^+(n, q) .$$

Our aim in the present section is to derive some more or less immediate consequences of these relations.

The presence of the factor q^{-n} in (3.4), (3.5) makes it much easier to estimate the c ratios than the s ratios. Indeed, on the basis of (3.4) – (3.7) alone, we can prove the existence of the limits

$$c_M(\infty, q) = \lim_{n \rightarrow \infty} c_M(n, q), \quad c_G(\infty, q) = \lim_{n \rightarrow \infty} c_G(n, q)$$

and give realistic estimates of the rates at which they are approached.

All four ratios $c_M(n, q), \dots$ have the value 1 when $n = 1$. It is easily checked that, when $n \geq 2$

$$(3.8) \quad 0 < s_M(n, q) < c_M(n, q) < 1,$$

$$(3.9) \quad 0 < s_G(n, q) < c_G(n, q) < 1.$$

LEMMA 3.1. *The sequence*

$$(3.10) \quad c_M(1, q), c_M(2, q), \dots$$

is strictly decreasing and so the limit $c_M(\infty, q)$ exists. If $n \geq 3$, we have

$$(3.11) \quad c_M(n-1, q) - c_M(n, q) < q^{-n} - q^{-n-3}$$

PROOF: Multiplying (3.4) through by $\omega(n, q)$ and using (3.6), we get

$$(3.12) \quad (c_M(n, q) - c_M(n-1, q))(1 - q^{-n}) = (s_M(n, q) - c_M(n, q))q^{-n}.$$

The first assertion of the Lemma now follows from (3.8).

Rearrangement of (3.12) gives

$$(3.13) \quad c_M(n, q) - c_M(n-1, q) = (s_M(n, q) - c_M(n-1, q))q^{-n}.$$

Assuming now that $n \geq 3$, and using (3.8) and the first part of the Lemma, we deduce from (3.13) that

$$\begin{aligned} c_M(n, q) - c_M(n-1, q) &> -c_M(n-1, q)q^{-n} \\ &\geq -c_M(2, q)q^{-n} \\ &= -(1 - q^{-3})q^{-n}, \end{aligned}$$

which is the second assertion of the Lemma. □

By summation we get from (3.11) the inequalities

$$(3.14) \quad 0 < c_M(d, q) - c_M(n, q) < \sum_{i=1}^3 q^{-d-i} \quad (n > d \geq 2),$$

$$(3.15) \quad 0 < c_M(n, q) - c_M(\infty, q) < \sum_{i=1}^3 q^{-n-i} \quad (n \geq 3).$$

EXAMPLE. Let $q = 2$. The Neumann–Praeger inequalities give in this case

$$1/12 < 1 - c_M(n, 2) < 1/3.$$

Calculating $c_M(m, 2)$ explicitly for $m \leq 5$ and using (3.14) with $d = 5$, we get the sharper bounds

$$\begin{aligned} \frac{1}{4} - \left(\frac{1}{2}\right)^{n+1} &\leq 1 - c_M(n, 2) < \frac{1}{4} \quad (2 \leq n \leq 5), \\ \frac{1}{4} - \frac{1}{64} &\leq 1 - c_M(n, 2) < \frac{1}{4} + \frac{1}{32} \quad (n > 5). \end{aligned}$$

Similar considerations hold for $c_G(n, q)$. The identity

$$(3.16) \quad c_G(n, q)\omega(n, q) - c_G(n-1, q)\omega(n-1, q) = \omega(n-1, q)(s_G(n, q) - c_G(n, q) - s_G(n-1, q))q^{-n}$$

and its rearrangement

$$(3.17) \quad c_G(n, q) - c_G(n-1, q) = (s_G(n, q) - s_G(n-1, q))q^{-n}$$

yield the following companion to Lemma 3.1. (Observe that the sequence $\omega(1, q), \omega(2, q), \dots$ has the *nonzero* limit $\omega(\infty, q) = \prod_{i=1}^{\infty} (1 - q^{-i})$.)

LEMMA 3.2. *The sequence*

$$(3.18) \quad c_G(1, q)\omega(1, q), c_G(2, q)\omega(2, q), \dots$$

is strictly decreasing and so the limit $c_G(\infty, q)$ exists. For $n \geq 1$, we have

$$(3.19) \quad |c_G(n, q) - c_G(n-1, q)| \leq q^{-n}.$$

By summation, we get

$$(3.20) \quad |c_G(n, q) - c_G(d, q)| \leq 1/q^d(q-1) \quad (1 \leq d \leq n \leq \infty).$$

REMARK. Unlike (3.10) and (3.18), the sequence

$$(3.21) \quad c_G(1, q), c_G(2, q), \dots$$

is by no means monotonic. By (3.5) and (3.7), $c_G(n, q) - c_G(n-1, q)$ has the same sign as $a^+(n, q) - a^+(n-1, q)$; but the consideration of the leading terms in Section 7 shows that the latter difference varies in sign in quite a complicated way as n increases.

4. FORM OF THE COEFFICIENTS

In the present section we look more closely at the coefficients $a(n, q), a^+(n, q)$. From (2.14) we derive the explicit formula

$$(4.1) \quad a(n, q) = \sum_{\lambda \vdash n} a(\lambda, q),$$

where summation is over the partitions

$$(4.2) \quad \lambda = (1^{r_1} 2^{r_2} \dots)$$

of n , and where

$$(4.3) \quad a(\lambda, q) = \frac{\binom{N_1}{r_1} \binom{N_2}{r_2} \dots}{(q-1)^{r_1} (q^2-1)^{r_2} \dots}.$$

Here, N_k is an abbreviation for $N(k, q)$ and we shall later write N_k^+ for $N^+(k, q)$.

The denominator in (4.3) is $q^n g_\lambda(q^{-1})$, where

$$(4.4) \quad g_\lambda(t) = \prod_d (1 - t^d)^{r_d}.$$

Using (2.8), we find that the numerator has the form $q^n f_\lambda(q^{-1}) z_\lambda^{-1}$, where

$$(4.5) \quad f_\lambda(t) \in \mathbb{Z}[t], f_\lambda(0) = 1,$$

and

$$(4.6) \quad z_\lambda = \prod_d d^{r_d} r_d!.$$

To be explicit, we have

$$dN_d = q^d f_d(q^{-1}),$$

where

$$(4.7) \quad f_d(t) = \sum_{\delta|d} \mu(d/\delta) t^{d-\delta},$$

and therefore

$$(4.8) \quad f_\lambda(t) = \prod_d f_d^{(r_d)}(t),$$

where

$$(4.9) \quad f_d^{(r)}(t) = \prod_{i=0}^{r-1} (f_d(t) - i t^d).$$

In conclusion,

$$(4.10) \quad a(n, q) = A_n(q^{-1}),$$

where

$$(4.11) \quad A_n(t) = \sum_{\lambda \vdash n} z_\lambda^{-1} f_\lambda(t) g_\lambda(t)^{-1}.$$

By a similar argument,

$$(4.12) \quad a^+(n, q) = A_n^+(q^{-1}),$$

where

$$(4.13) \quad A_n^+(t) = \sum_{\lambda \vdash n} z_\lambda^{-1} f_\lambda^+(t) g_\lambda(t)^{-1},$$

and $f_\lambda^+(t)$ also has the properties (4.5). Indeed, $f_\lambda^+(t)$ is defined in exactly the same way as $f_\lambda(t)$, except that $f_1(t) (= 1)$ is to be replaced at every occurrence by $f_1^+(t) = 1 - t$. Thus, $f_\lambda^+(t) = f_{(1, \lambda)}(t)$, where, if $\lambda = (1^{r_1} 2^{r_2} \dots) \vdash n$, then $(1, \lambda) = (1^{r_1+1} 2^{r_2} \dots) \vdash n+1$. Notice that, since (4.10), (4.12) hold for all prime-powers q , the rational functions $A_n(t), A_n^+(t)$ appearing in them are uniquely determined.

Since $f_\lambda(0) = f_\lambda^+(0) = g_\lambda(0) = 1$ and since $n!z_\lambda^{-1}$ is the number of elements of the symmetric group S_n of cycle type λ , it follows that

$$(4.14) \quad A_n(0) = A_n^+(0) = 1.$$

Thus, the series $1/(1 - u) = \sum_n u^n$ is the common limiting form of the two series $P(q, u), P^+(q, u)$ as $q \rightarrow \infty$.

Let us now consider the denominator of $A_n(t)$. Write

$$(4.15) \quad \Omega_n(t) = \prod_{i=1}^n (1 - t^i),$$

so that, in our earlier notation,

$$(4.16) \quad \omega(m, q) = \Omega_n(q^{-1}).$$

LEMMA 4.1. $\Omega_m(t)\Omega_n(t) \mid \Omega_{m+n}(t)$.

PROOF: All the irreducible factors of $\Omega_k(t)$ in $\mathbb{Q}[t]$ are cyclotomic polynomials $\Phi_r(t)$. It is therefore sufficient to prove that $\Phi_r(t)$ divides $\Omega_{m+n}(t)$ to at least as high a power as it divides $\Omega_m(t)\Omega_n(t)$. But $\Phi_r(t)$ divides $\Omega_k(t)$ precisely to the power $[k/r]$, and we have the simple inequality $[(m+n)/r] \geq [m/r] + [n/r]$. □

COROLLARY 4.2. $\Omega_n(t)$ is the least common multiple of the $g_\lambda(t)$ with $\lambda \vdash n$.

PROOF: It follows easily from the Lemma that $\Omega_n(t)$ is a common multiple of the $g_\lambda(t)$. On the other hand, if r is any integer > 0 and a, b are the quotient and remainder on dividing n by r , then $\Phi_r(t)^a \parallel \Omega_n(t)$ and $\Phi_r(t)^a \mid g_\lambda(t)$, where $\lambda = (br^a) \vdash n$. \square

The Corollary shows that the rational functions

$$(4.17) \quad K_n(t) := A_n(t)\Omega_n(t),$$

$$(4.18) \quad K_n^+(t) := A_n^+(t)\Omega_n(t)$$

are in fact polynomials. Explicitly, we have by (4.11), (4.13),

$$(4.19) \quad K_n(t) = \sum_{\lambda \vdash n} z_\lambda^{-1} f_\lambda(t) h_\lambda(t),$$

$$(4.20) \quad K_n^+(t) = \sum_{\lambda \vdash n} z_\lambda^{-1} f_\lambda^+(t) h_\lambda(t),$$

where

$$(4.21) \quad h_\lambda(t) = \Omega_n(t)/g_\lambda(t).$$

These considerations imply

PROPOSITION 4.3. $a(n, q)\omega(n, q)$ and $a^+(n, q)\omega(n, q)$, and hence also $s_M(n, q)$, $c_M(n, q)$, $s_G(n, q)\omega(n, q)$ and $c_G(n, q)\omega(n, q)$, are polynomials in q^{-1} with rational coefficients.

Lehrer [1] arrives at formulae equivalent to (4.11), (4.13) by a quite different method. Interpreting the right hand sides of (4.19), (4.20) as inner products of generalised characters of the symmetric group S_n (with coefficients in $\mathbb{Z}[t]$ rather than \mathbb{Z}), he deduces the more subtle result that the polynomials in Proposition 4.3 have *integral* coefficients.

I am indebted to the referee for pointing out the following

COROLLARY 4.4. The numbers of cyclic and separable elements in $M(n, q)$ and $GL(n, q)$ are polynomials in q .

PROOF: These numbers are obtained by multiplying the ratios in Proposition 4.3 by $|GL(n, q)| = q^{n^2}$. However, as is easily checked, the ratios are polynomials in q^{-1} of degree at most n^2 . \square

5. COMPLEX FUNCTIONS

In Section 3, using quite simple arguments, we proved the existence of the limits $c_M(\infty, q)$, $c_G(\infty, q)$ and derived estimates of the rates at which they are approached.

Proving corresponding results for the s ratios is harder. For this purpose, and in order to evaluate all four limits explicitly, we need to look at $P(q, z)$ as an analytic function of a complex variable z .

The transition from formal power series to analytic functions is governed by standard general principles. Suppose we are given a formally convergent infinite product

$$(5.1) \quad \prod_{d=1}^{\infty} (1 + u_d(t))^{m_d},$$

where the $u_d(t)$ are rational functions of t and the m_d positive integers, and that we are required to show that the corresponding functional product

$$(5.2) \quad \prod_{d=1}^{\infty} (1 + u_d(z))^{m_d}$$

is analytic in a given open disc

$$D(R) = \{z \mid |z| < R\},$$

where $R > 0$. This comes to showing that (5.2) is uniformly absolutely convergent in every closed disc

$$\bar{D}(r) = \{z \mid |z| \leq r\},$$

where $r < R$. The condition for this, obtained by applying Weierstrass' M-test to (5.2) written out at length as a product of individual terms $1 + u_d(z)$, is that there exist a constant $b = b(r)$ such that

$$(5.3) \quad \sum_{d=0}^{\infty} m_d |u_d(z)| \leq b \text{ for all } z \in \bar{D}(r).$$

When this condition is satisfied, (5.2) will be analytic in $D(R)$ and the formal power series expansion of (5.1) will be its Taylor series at $z = 0$.

It follows from these principles that the complex function $P(q, z)$ corresponding to the formal infinite $P(q, t)$ is analytic for $|z| < 1$. Indeed, the sum in (5.3) is

$$\sum_{d=1}^{\infty} N(d, q) |z|^d / (q^d - 1) = \frac{q}{q-1} |z| + \sum_{d=2}^{\infty} N(d, q) |z|^d / (q^d - 1),$$

and the inequality $N(d, q) \leq q^d - 1$ ($d \geq 2$) shows that this is at most $qr / (q - 1) + r^2 / (1 - r)$ when $|z| \leq r < 1$.

By a similar argument,

$$(5.4) \quad 1 - z = \prod_{d=1}^{\infty} (1 - z^d/q^d)^{N(d,q)}$$

when $|z| < 1$. Replacing z by $q(z/q)^m$, where m is a positive integer, we get the slightly more general result that

$$(5.5) \quad 1 - q(z/q)^m = \prod_{d=1}^{\infty} (1 - z^{md}/q^{md})^{N(d,q)}$$

for $|z| < q^{1-1/m}$ and a fortiori for $|z| < 1$.

The central result of the present section is that, apart from a simple pole at $z = 1$, $P(q, z)$ can be continued analytically over the disc $|z| < q$. This depends on two simple identities:

$$(5.6) \quad \left(1 - \frac{z^d}{q^d}\right) \left(1 + \frac{z^d}{q^d - 1}\right) = 1 - \frac{z^d(z^d - 1)}{q^d(q^d - 1)},$$

$$(5.7) \quad \left(1 + \frac{z^d}{q^d}\right)^{-1} \left(1 + \frac{z^d}{q^d - 1}\right) = 1 + \frac{1}{(q^d - 1)} \left(\frac{(z/q)^d}{1 + (z/q)^d}\right).$$

PROPOSITION 5.1. *The function*

$$(5.8) \quad T(q, z) = \prod_{d=1}^{\infty} \left(1 + \frac{1}{(q^d - 1)} \left(\frac{(z/q)^d}{1 + (z/q)^d}\right)\right)^{N(d,q)}$$

is analytic in $D(q)$ and equal to

$$(5.9) \quad (1 - z^2/q)^{-1} (1 - z)P(q, z)$$

in $D(1)$.

PROOF: Let $|z| \leq qr < q$. Then the sum (5.3) corresponding to $T(q, z)$ is at most

$$\frac{q}{q-1} \cdot \frac{r}{1-r} + \sum_{d=2}^{\infty} \frac{r^d}{1-r} = \frac{q}{q-1} \cdot \frac{r}{1-r} + \frac{r^2}{(1-r)^2}.$$

This proves the first statement.

Suppose now that $|z| < 1$. By (5.7),

$$P(q, z) = T(q, z) \prod_{d=1}^{\infty} (1 + z^d/q^d)^{N(d,q)}.$$

Then, using (5.4) and (5.5), we get

$$\begin{aligned} (1 - z)P(q, z) &= T(q, z) \prod_{d=1}^{\infty} (1 - z^{2d}/q^{2d})^{N(d,q)} \\ &= T(q, z)(1 - z^2/q), \end{aligned}$$

which proves the second statement. □

REMARK. The condition that the typical term in (5.8) be zero reduces to $z^d + q^d = 1$. Accordingly, every point on the circle $|z| = q$ is a limit point of zeros of $T(q, z)$, and so this circle is a natural boundary for $T(q, z)$.

PROPOSITION 5.2. *The function*

$$(5.10) \quad P(q, z) - 1/(1 - z),$$

analytic in $D(1)$, can be continued analytically over $D(q)$.

PROOF: By the Proposition above, the function $S(q, z) = (1 - z^2/q)T(q, z)$ is analytic in $D(q)$ and equal to $(1 - z)P(q, z)$ in $D(1)$. Therefore the function $R(q, z)$ defined by

$$R(q, z) = \begin{cases} \frac{S(q, z) - S(q, 1)}{z - 1} & \text{if } z \neq 1, \\ S'(q, 1) & \text{if } z = 1, \end{cases}$$

is analytic in $D(q)$ and equal to $-(P(q, z) - S(q, 1)/(1 - z))$ in $D(1)$. Thus, we have only to prove that

$$(5.11) \quad S(q, 1) = 1.$$

Now, for $z \in D(1)$,

$$(5.12) \quad \begin{aligned} S(q, z) &= \prod_{d=1}^{\infty} \left[(1 - z^d/q^d)(1 + z^d/(q^d - 1)) \right]^{N(d, q)} \\ &= \prod_{d=1}^{\infty} \left(1 - \frac{z^d(z^d - 1)}{q^d(q^d - 1)} \right)^{N(d, q)} \end{aligned}$$

by (5.6). But (5.12) remains valid in $D(q^{1/2})$ because, by the usual arguments, the right hand side represents an analytic function in that region. Putting $z = 1$ in (5.12), we get the required result (5.11). □

COROLLARY 5.3. *If $0 \leq r < q$,*

$$(5.13) \quad \lim_{n \rightarrow \infty} (a(n, q) - 1)r^n = 0,$$

and in particular

$$(5.14) \quad \lim_{n \rightarrow \infty} a(n, q) = 1.$$

PROOF: The Taylor series $\sum_{n=0}^{\infty} (a(n, q) - 1)t^n$ of $P(q, z) - 1/(1 - z)$ at $z = 0$, being also that of $-R(q, z)$, has radius of convergence q . □

The corresponding results for $P^+(q, z)$ are that

$$(5.15) \quad P^+(q, z) - (1 - q^{-1})/(1 - z)$$

can be continued analytically over $D(q)$ and that

$$(5.16) \quad \lim_{n \rightarrow \infty} a^+(n, q) = 1 - q^{-1} .$$

One more result is required in order to evaluate the limits in the next section.

PROPOSITION 5.4. $P(q, q^{-1}) = (1 - q^{-5})/(1 - q^{-1})(1 - q^{-2})$.

PROOF: Putting $z = q^{-1}$ in (5.12) and using (5.5), we get

$$\begin{aligned} (1 - q^{-1})P(q, q^{-1}) &= \prod_{d=1}^{\infty} \left(1 - \frac{q^{-d}(q^{-d} - 1)}{q^d(q^d - 1)} \right)^{N(d, q)} \\ &= \prod_{d=1}^{\infty} (1 + q^{-3d})^{N(d, q)} \\ &= \prod_{d=1}^{\infty} \left(\frac{1 - q^{-6d}}{1 - q^{-3d}} \right)^{N(d, q)} \\ &= (1 - q^{-5})/(1 - q^{-2}) . \end{aligned}$$

□

6. NUMERICAL LIMITS AND ESTIMATES

In Section 3, we proved the existence of the limits of the c ratios as $n \rightarrow \infty$ and gave estimates of the rates at which they are approached. Here we do the same for the s ratios. We also evaluate all four limits explicitly.

The limit of $\omega(n, q)$ as $n \rightarrow \infty$ is evidently

$$(6.1) \quad \omega(\infty, q) = \Omega(q^{-1}) ,$$

where

$$(6.2) \quad \Omega(t) = \prod_{i=1}^{\infty} (1 - t^i) .$$

By Euler's pentagonal number theorem,

$$(6.3) \quad \Omega(t) = 1 + \sum_{n=1}^{\infty} (-1)^n \left(t^{1/2n(3n-1)} + t^{1/2n(3n+1)} \right) .$$

The crucial results in determining the limits of the s ratios are (5.14) and (5.16). These, together with (3.6) and (3.7), show immediately that the limits exist and have the values

$$(6.4) \quad s_G(\infty, q) = 1 - q^{-1},$$

$$s_M(\infty, q) = \omega(\infty, q)$$

$$(6.5) \quad = 1 - q^{-1} - q^{-2} + q^{-5} + q^{-7} - q^{-12} - q^{-15} + \dots.$$

Estimating the rates at which these limits are approached is more difficult. This comes down to estimating $|a(n, q) - 1|$ and $|a^+(n, q) - 1 + q^{-1}|$. Now, by Proposition 5.2,

$$1 = \lim_{z \rightarrow 1} (1 - z)P(q, z) = \sum_{i=0}^{\infty} (a(i, q) - a(i - 1, q)),$$

whence, for all n ,

$$(6.6) \quad a(n, q) - 1 = - \sum_{i=n+1}^{\infty} (a(i, q) - a(i - 1, q)).$$

We shall make use of the resulting inequality

$$(6.7) \quad |a(n, q) - 1| \leq \sum_{i=n+1}^{\infty} |a(i, q) - a(i - 1, q)|.$$

The corresponding results for $a^+(n, q)$ are

$$(6.8) \quad a^+(n, q) - 1 + q^{-1} = - \sum_{i=n+1}^{\infty} (a^+(i, q) - a^+(i - 1, q)),$$

$$(6.9) \quad |a^+(n, q) - 1 + q^{-1}| \leq \sum_{i=n+1}^{\infty} |a^+(i, q) - a^+(i - 1, q)|.$$

NOTATION. For formal power series $A(t) = \sum \alpha_n t^n$, $B(t) = \sum \beta_n t^n$ with real coefficients. $A(t) \ll B(t)$ means that $\alpha_n \leq \beta_n$ for all n .

We recall that

$$(6.10) \quad \Omega(t)^{-1} = \sum_{n=0}^{\infty} p(n)t^n,$$

where $p(n)$ is the number of partitions of n .

PROPOSITION 6.1. *We have*

$$(6.11) \quad \sum_{n=0}^{\infty} |a(n, q) - a(n - 1, q)| q^n t^n \ll \left(\frac{1}{1-t} + qt^2 \right) \Omega(t)^{-1}.$$

Thus, for all n ,

$$(6.12) \quad |a(n, q) - a(n - 1, q)| q^n \leq p_2(n) + qp(n - 2),$$

where $p_2(n) = \sum_{i=0}^n p(i)$.

PROOF: The formal identity behind Proposition 5.1 is

$$(1 - qt)P(q, qt) = (1 - qt^2) \prod_{d=1}^{\infty} \left(1 + \frac{1}{q^d - 1} \cdot \frac{t^d}{1 + t^d} \right)^{N(d, q)},$$

from which we get

$$(6.13) \quad \sum_{n=0}^{\infty} (a(n, q) - a(n - 1, q)) q^n t^n = \left(\sum \gamma_n t^n \right) \prod_{d=1}^{\infty} \left(1 + \frac{1}{q^d - 1} \cdot \frac{t^d}{1 + t^d} \right)^{N^+(d, q)}$$

where

$$\sum \gamma_n t^n = (1 - qt^2) \left(1 + \frac{1}{q-1} \cdot \frac{t}{1+t} \right).$$

Expanding each factor on the right of (6.13) in powers of t and then formally multiplying all the factors together, we may express $(a(n, q) - a(n - 1, q)) q^n t^n$ as a sum of terms of the form

$$(\gamma_i t^i) \cdots \left(\pm \frac{t^{md}}{q^d - 1} \right) \cdots$$

Forming the corresponding sum of terms

$$(|\gamma_i| t^i) \cdots \left(+ \frac{t^{md}}{q^d - 1} \right) \cdots,$$

we conclude that

$$\sum_{n=0}^{\infty} |a(n, q) - a(n - 1, q)| q^n t^n \ll \left(\sum |\gamma_n| t^n \right) \prod_{d=1}^{\infty} \left(1 + \frac{1}{q^d - 1} \frac{t^d}{1 - t^d} \right)^{N^+(d, q)}.$$

It is easily verified that

$$\sum |\gamma_n| t^n \ll \frac{1}{1-t} + qt^2.$$

Also, since $(1 + (t/m))^m \ll e^t$ when m is a positive integer and since, by (2.7), $dN^+(d, q) \leq q^d - 1$, we have

$$\left(1 + \frac{1}{q^d - 1} \cdot \frac{t^d}{1 - t^d}\right)^{N^+(d, q)} \ll \exp\left(\frac{N^+(d, q)}{q^d - 1} \cdot \frac{t^d}{1 - t^d}\right) \ll \exp\left(\frac{1}{d} \frac{t^d}{1 - t^d}\right)$$

Putting all these results together, we deduce finally that

$$\begin{aligned} \sum_{n=0}^{\infty} |a(n, q) - a(n - 1, q)| q^n t^n &\ll \left(\frac{1}{1 - t} + qt^2\right) \exp\left(\sum_{d=1}^{\infty} \frac{1}{d} \sum_{m=1}^{\infty} t^{md}\right) \\ &= \left(\frac{1}{1 - t} + qt^2\right) \exp\left(\sum_{m=1}^{\infty} \sum_{d=1}^{\infty} \frac{t^{md}}{d}\right) \\ &= \left(\frac{1}{1 - t} + qt^2\right) \Omega(t)^{-1}, \end{aligned}$$

as required. □

COROLLARY 6.2. *For all n ,*

$$(6.14) \quad |a(n, q) - 1| \leq \sum_{d=n+1}^{\infty} (p_2(d) + qp(d - 2))q^{-d}.$$

More convenient (but weaker) versions of (6.14) can be derived as follows. Given c such that $1 < c < q$, we may choose k so that $p(n) \leq kc^n$ for all n . We have then also

$$p_2(n) \leq k \left(\frac{c^{n+1} - 1}{c - 1}\right) < \left(\frac{kc}{c - 1}\right) c^n.$$

Using these inequalities in (6.14), we conclude that

$$(6.15) \quad |a(n, q) - 1| \leq K(q/c)^{-n},$$

where

$$(6.16) \quad K = k \left(\frac{c}{c - 1} + \frac{q}{c^2}\right) \left(\frac{c}{q - c}\right).$$

EXAMPLES. Since $p(n) \leq 2^{n-1}$, we may take $c = 2$, $k = 1/2$, getting

$$(6.14) \quad |a(n, q) - 1| \leq \frac{1}{4} \left(\frac{q + 8}{q - 2}\right) \left(\frac{1}{2}q\right)^{-n},$$

provided that $q > 2$. The choice $c = 3/2$, $k = 1$ gives

$$(6.18) \quad |a(n, q) - 1| \leq \frac{1}{3} \left(\frac{4q + 27}{2q - 3}\right) \left(\frac{2}{3}q\right)^{-n}$$

for all q .

The corresponding results for $a^+(n, q)$ are that

$$(6.19) \quad |a^+(n, q) - 1 + q^{-1}| \leq \sum_{d=n+1}^{\infty} (p_2(d) + (q - 2)p_2(d - 2))q^{-d}$$

and

$$(6.20) \quad |a^+(n, q) - 1 + q^{-1}| \leq K^+(q/c)^{-n},$$

where

$$(6.21) \quad K^+ = \frac{kc}{c-1} \left(1 + \frac{q-2}{c^2}\right) \left(\frac{c}{q-c}\right).$$

The above results already give estimates for $|s_G(n, q) - s_G(\infty, q)| = |a^+(n, q) - 1 + q^{-1}|$. In the other case, we have, for example,

$$(6.22) \quad |s_M(n, q) - s_M(\infty, q)| \leq |a(n, q) - 1| + 1/q^n(q - 1),$$

as is easily checked.

REMARKS. The values of the first few $a(n, q), a^+(n, q)$ set down in Section 2, as well as our later estimates in the sense of the formal norm $\|\cdot\|_q$, indicate that the above estimates fail to mirror the true situation. It is a deficiency of our method that it takes no account of the many changes of sign of $a(n, q) - a(n - 1, q)$ as n increases (see Section 7). The estimates in the sense of $\|\cdot\|_q$ probably give a truer picture.

We turn now to the limiting values of the c ratios. The crucial result here is Proposition 5.4. It follows from (3.4), (3.5) that

$$c_M(n, q) = \omega(n, q) \sum_{i=0}^n a(i, q)q^{-i},$$

$$c_G(n, q) = \sum_{i=0}^n (a^+(i, q) - a^+(i - 1, q))q^{-i},$$

whence

$$c_M(\infty, q) = \omega(\infty, q)P(q, q^{-1}),$$

$$c_G(\infty, q) = [(1 - u)P^+(q, u)]_{u=q^{-1}}$$

$$= \frac{(1 - q^{-1})}{(1 + q^{-1}/(q - 1))} P(q, q^{-1}).$$

Using Proposition 5.4 and simplifying, we get

$$\begin{aligned}
 c_M(\infty, q) &= (1 - q^{-5}) \prod_{i=3}^{\infty} (1 - q^{-i}) \\
 (6.23) \qquad &= 1 - q^{-3} - q^{-4} - 2q^{-5} - q^{-6} + q^{-8} + 2q^{-9} + 2q^{-10} \dots,
 \end{aligned}$$

$$\begin{aligned}
 c_G(\infty, q) &= (1 - q^{-5}) (1 + q^{-3})^{-1} \\
 (6.24) \qquad &= 1 - q^{-3} - q^{-5} + q^{-6} + q^{-8} - q^{-9} \dots.
 \end{aligned}$$

REMARKS.

- (1) Although q^{-3} is a simple improvement on the Neumann–Praeger *lower* bound for $1 - c_M(n, q)$ in (1.1), their *upper* bound, namely $q^{-3} + q^{-4} + 2q^{-5} + 2q^{-6} \dots$, is remarkably close to the limiting value given by (6.23).
- (2) By inspection, $s_M(\infty, q)/\omega(\infty, q)$, $c_M(\infty, q)/\omega(\infty, q)$, $s_G(\infty, q)$ and $c_G(\infty, q)$ are polynomials in q^{-1} , in strange contrast with Proposition 4.3.

In Section 3, we gave estimates of the rates at which the c ratios approach their limiting values. The results just obtained shed further light on the matter. Indeed, by (3.13),

$$\begin{aligned}
 \lim_{n \rightarrow \infty} (c_M(n - 1, q) - c_M(n, q))q^{n+1} \\
 &= q(c_M(\infty, q) - s_M(\infty, q)) \\
 &= \omega(\infty, q) (qP(q, q^{-1}) - 1) \\
 (6.25) \qquad &= 1 + q^{-1} - q^{-2} - q^{-3} - 3q^{-4} \dots,
 \end{aligned}$$

and similarly, by (3.16),

$$\begin{aligned}
 \lim_{n \rightarrow \infty} (c_G(n - 1, q) \omega(n - 1, q) - c_G(n, q)\omega(n, q))q^n \\
 &= \omega(\infty, q)c_G(\infty, q) \\
 (6.26) \qquad &= 1 - q^{-1} - q^{-2} - q^{-3} + q^{-4} \dots
 \end{aligned}$$

7. FORMAL ESTIMATES

We have so far only considered limits in the sense of the ordinary absolute value $|\cdot|$. We turn now to limits in the sense of the formal norm $\|\cdot\|_q$.

It was shown in Section 4 that $a(n, q) = A_n(q^{-1})$ for all prime-powers q , where $A_n(t)$ is a uniquely determined rational function whose poles all lie on the unit circle. Thus, there is a power series expansion

$$(7.1) \qquad A_n(z) - 1 = \sum_{m=0}^{\infty} \alpha_{nm} z^m,$$

valid for $|z| < 1$. If $\alpha_{nr}z^r$ is the leading term (so that $\alpha_{nr} \neq 0$ but $\alpha_{nm} = 0$ for $m < r$), then, by definition,

$$(7.2) \quad \|a(n, q) - 1\|_q = q^{-r}.$$

PROPOSITION 7.1. $\|a(n, q) - 1\|_q \leq q^{-n}$.

PROOF: The leading coefficient is given by

$$\alpha_{nr} = \lim_{z \rightarrow 0} (A_n(z) - 1)z^{-r}.$$

On the other hand, by (6.15) there is a constant e such that

$$|A_n(q^{-1}) - 1| \leq eq^{-n}$$

for all prime-powers q . These results together show that $r \geq n$. □

The same argument gives

PROPOSITION 7.2. $\|a^+(n, q) - 1 + q^{-1}\|_q \leq q^{-n}$.

These two results show that $a(n, q)$, $a^+(n, q)$ tend *formally* to their *numerical* limits 1 , $1 - q^{-1}$ as $n \rightarrow \infty$. The same applies to the c and s ratios: for, besides $a(n, q)$, $a^+(n, q)$, the only other functions whose limits are involved are $\omega(n, q)$ and the n^{th} partial sum of $P(q, q^{-1})$; and in these cases, the numerical limits are obviously the formal ones as well.

Lehrer [1, Proposition (8.6)] proves the formal convergence of the sequence $s_M(1, q), s_M(2, q), \dots$ by showing that

$$\|s_M(m, q) - s_M(n, q)\|_q \leq q^{-\lfloor n/2 \rfloor}$$

whenever $m \leq n$. The results above show that the formal limit is $s_M(\infty, q) = \omega(\infty, q)$ and that

$$\|s_M(n, q) - \omega(\infty, q)\|_q \leq q^{-n}.$$

EXAMPLE. Let $m_n = m_n(q) = 1 - c_M(n, q)$. It was shown in Section 4 that m_n is a polynomial in q^{-1} and in Section 6 that

$$\begin{aligned} \lim_{n \rightarrow \infty} m_n &= q^{-3} + q^{-4} + 2q^{-5} + q^{-6} \dots; \\ \lim_{n \rightarrow \infty} (m_n - m_{n-1})q^{n+1} &= 1 + q^{-1} - q^{-2} - q^{-3} - 3q^{-4} \dots. \end{aligned}$$

The formal versions of these limits are illustrated in the following table of values. The entries in the row labelled $m_r - m_{r-1}$ or m_r are the coefficients of q^{-3}, q^{-4}, \dots , and k' stands for $-k$. For example, $m_3 - m_2 = q^{-4} + q^{-5} - q^{-6} - q^{-7}$.

$$\begin{array}{l}
 m_2 - m_1 \quad 1 \\
 m_3 - m_2 \quad 0 \quad 1 \quad 1 \quad 1' \quad 1' \\
 m_4 - m_3 \quad 0 \quad 0 \quad 1 \quad 1 \quad 1' \quad 2' \quad 2' \quad 1 \quad 1 \quad 1 \\
 m_5 - m_4 \quad 0 \quad 0 \quad 0 \quad 1 \quad 1 \quad 1' \quad 1' \quad 3' \quad 1' \quad 2 \quad 3 \quad 3 \quad 0 \quad 1' \quad 2' \quad 1' \\
 \\
 m_1 = 0 \\
 m_2 \quad 1 \\
 m_3 \quad 1 \quad 1 \quad 1 \quad 1' \quad 1' \\
 m_4 \quad 1 \quad 1 \quad 2 \quad 0 \quad 2' \quad 2' \quad 2' \quad 1 \quad 1 \quad 1 \\
 m_5 \quad 1 \quad 1 \quad 2 \quad 1 \quad 1' \quad 3' \quad 3' \quad 2' \quad 0 \quad 3 \quad 3 \quad 3 \quad 0 \quad 1' \quad 2' \quad 1'
 \end{array}$$

Let us consider, for fixed n , the leading term $\alpha_{nr}q^{-r}$ of $a(n, q) - 1$. Since

$$\lim_{q \rightarrow \infty} (a(n, q) - 1) / \alpha_{nr}q^{-r} = 1,$$

it gives a good approximation to, and in particular has the same sign as, $a(n, q) - 1$ for sufficiently large q . In what follows, we shall determine $\alpha_{nr}q^{-r}$ explicitly for most values of n . The results almost certainly give more accurate information about $a(n, q) - 1$ than the earlier numerical estimates. They suggest, for example, that (for fixed q) it assumes both positive and negative values for infinitely many n . Similar results hold for $a^+(n, q) - 1 + q^{-1}$, although these will be presented in less detail.

As before, (6.6) will be used to investigate $a(n, q) - 1$. Thus, we need to examine the series

$$(1 - t)P(q, t) = \sum_{n=0}^{\infty} (a(n, q) - a(n - 1, q))t^n.$$

Our consideration are purely formal and no questions of (numerical) convergence arise.

Taking logarithms in (2.14), we get

$$\begin{aligned}
 \log[(1 - t)P(q, t)] &= - \sum_{n=1}^{\infty} \frac{t^n}{n} + \sum_{d=1}^{\infty} N(d, q) \log \left(1 + \frac{t^d}{q^d - 1} \right) \\
 &= - \sum_{n=1}^{\infty} \frac{t^n}{n} + \sum_{d=1}^{\infty} dN(d, q) \sum_{m=1}^{\infty} \frac{(-1)^{m+1}}{md} \frac{t^{md}}{(q^d - 1)^m} \\
 &= \sum_{n=1}^{\infty} b'_n \frac{t^n}{n},
 \end{aligned}$$

where

$$\begin{aligned} b'_n &= -1 - \sum_{d|n} dN(d, q) \frac{(-1)^{n/d}}{(q^d - 1)^{n/d}} \\ &= -1 - \sum_{\substack{\delta|d|n \\ \delta < n}} \mu(d/\delta) \frac{q^\delta (-1)^{n/d}}{(q^d - 1)^{n/d}} \\ &= \frac{1}{q^n - 1} - \sum_{\substack{\delta|d|n \\ \delta < n}} \mu(d/\delta) \frac{q^\delta (-1)^{n/d}}{(q^d - 1)^{n/d}}. \end{aligned}$$

Thus, writing $b'_n = b_n q^{-n}$, we get

$$(7.3) \quad \log [(1 - t)P(q, t)] = \sum_{n=1}^{\infty} \frac{b_n}{n} \left(\frac{t}{q}\right)^n,$$

where

$$(7.4) \quad b_n = \frac{1}{1 - q^{-n}} - \sum_{\substack{\delta|d|n \\ \delta < n}} \mu(d/\delta) \frac{q^\delta (-1)^{n/d}}{(1 - q^{-d})^{n/d}}.$$

From (7.4), we may expand b_n as a Laurent series in q^{-1} . The coefficient of q^m , $m > 0$, is 0 unless $m | n$ and $m < n$, in which case it is $-\theta(n/m)$, where $\theta(k) = \sum_{d|k} \mu(d)(-1)^{k/d}$. The Möbius inversion formula shows that θ satisfies the summation formula $\sum_{d|k} \theta(d) = (-1)^k$, from which one sees that

$$\theta(1) = -1, \theta(2) = 2, \theta(k) = 0 \quad (k > 2).$$

It follows that b_n has the form

$$b_n = \begin{cases} \sum_{k=0}^{\infty} b_{nk} q^{-k} & (n \text{ odd}) \\ -2q^{n/2} + \sum_{k=0}^{\infty} b_{nk} q^{-k} & (n \text{ even}) \end{cases}$$

where

$$(7.6) \quad \sum_{k=0}^{\infty} b_{nk} q^{-k} = (1 - q^{-n})^{-1} - \sum_{\substack{\delta|d|n \\ \delta < n}} \mu(d/\delta) q^\delta (-1)^{n/d} [(1 - q^{-d})^{-n/d} - 1].$$

We require here only the first two coefficients in (7.6). By inspection,

$$(7.7) \quad b_{n0} = \sum_{d|n} (-1)^{d+1} d = \tau(n), \text{ say,}$$

$$(7.8) \quad b_{n1} = \begin{cases} (-1)^{n+1} \binom{n+1}{2} & (n \text{ odd}), \\ (-1)^{n/2 + (\frac{1}{2}n)+} (-1)^{n+1} \binom{n+1}{2} & (n \text{ even}). \end{cases}$$

Let us now express $(1 - t)P(q, t)$ and its logarithm in the form

$$(7.9) \quad (1 - t)P(q, t) = \mathcal{A}_- + \sum_{r=0}^{\infty} \mathcal{A}_r,$$

$$(7.10) \quad \log [(1 - t)P(q, t)] = \mathcal{B}_- + \sum_{r=0}^{\infty} \mathcal{B}_r,$$

where $\mathcal{A}_r, \mathcal{B}_r$ are formal \mathbb{Q} -linear combinations of terms $q^{-r}(t/q)^m$ and $\mathcal{A}_-, \mathcal{B}_-$ formal \mathbb{Q} -linear combinations of terms $q^s(t/q)^m$ with $s > 0$. Then

$$(7.11) \quad \mathcal{A}_- + \sum_{r=0}^{\infty} \mathcal{A}_r = (\exp \mathcal{B}_-) \prod_{r=0}^{\infty} (\exp \mathcal{B}_r).$$

We wish to calculate $\mathcal{A}_-, \mathcal{A}_0$ and for this purpose need to know $\exp \mathcal{B}_-, \exp \mathcal{B}_0$ and \mathcal{B}_1 . First,

$$\mathcal{B}_- = \sum_{n=1}^{\infty} -\frac{2q^m t^{2m}}{2mq^{2m}} = \log \left(1 - \frac{t^2}{q} \right).$$

whence

$$(7.12) \quad \exp \mathcal{B}_- = 1 - t^2/q.$$

Next,

$$\begin{aligned} \mathcal{B}_0 &= \sum_{m=1}^{\infty} \frac{\tau(m)}{m} (t/q)^m \\ &= \sum_{m=1}^{\infty} \sum_{d|m} (-1)^{d+1} \frac{d}{m} (t/q)^m \\ &= \sum_{d=1}^{\infty} (-1)^{d+1} \sum_{r=1}^{\infty} \frac{1}{r} (t/q)^{dr} \\ &= \sum_{d=1}^{\infty} (-1)^d \log (1 - t^d/q^d), \end{aligned}$$

whence

$$(7.13) \quad \exp B_0 = \Psi(t/q) ,$$

where

$$(7.14) \quad \Psi(t) = \frac{(1-t^2)(1-t^4)\dots}{(1-t)(1-t^3)\dots} .$$

By a well known theorem of Euler,

$$(7.15) \quad \begin{aligned} \Psi(t) &= \sum_{n=0}^{\infty} t^{n(n+1)/2} \\ &= 1 + t + t^3 + t^6 + t^{10} + \dots . \end{aligned}$$

Finally,

$$(7.16) \quad \begin{aligned} B_1 &= \sum_{n=1}^{\infty} (-1)^{n+1} \frac{\binom{n+1}{2}}{n} \frac{t^n}{q^{n+1}} + \sum_{m=1}^{\infty} (-1)^m \frac{m}{2m} \frac{t^{2m}}{q^{2m+1}} \\ &= \frac{1}{2q} \sigma(t/q) , \end{aligned}$$

where

$$(7.17) \quad \sigma(t) = (1+t^2)^{-1} - (1+t)^{-2} .$$

Denoting equality modulo $\sum_{r=1}^{\infty} \mathcal{A}_r$ by \sim , we have

$$\begin{aligned} \mathcal{A}_- + \mathcal{A}_0 &\sim (\exp B_-)(\exp B_0) \left(\exp \sum_{r=1}^{\infty} B_r \right) \\ &= (1-t^2/q) \Psi(t/q) \left(\exp \sum_{r=1}^{\infty} B_r \right) \\ &\sim (1-t^2/q) \Psi(t/q) \left(1 + \frac{1}{2q} \sigma(t/q) \right) , \end{aligned}$$

and so

$$(7.18) \quad \mathcal{A}_- = -(t^2/q) \Psi(t/q) ,$$

$$(7.19) \quad \mathcal{A}_0 = \left(1 - \frac{1}{2} (t^2/q^2) \sigma(t/q) \right) \Psi(t/q) .$$

Let $T(m)$ denote the m^{th} triangular number :

$$(7.20) \quad T(m) = \frac{1}{2}m(m + 1) \quad (m = 0, 1, \dots)$$

Then, by (7.15) and (7.18), we have

$$(7.21) \quad \mathcal{A}_- = \sum_{n=0}^{\infty} \lambda_n \frac{t^n}{q^{n-1}},$$

where

$$(7.22) \quad \lambda_n = \begin{cases} -1 & \text{if } n = T(m) + 2, \\ 0 & \text{otherwise.} \end{cases}$$

Thus, by (7.19),

$$(7.23) \quad a(n, q) - a(n - 1, q) = \lambda_n q^{-(n-1)} + \phi_n q^{-n} + \dots,$$

where

$$(7.24) \quad \sum_{n=0}^{\infty} \phi_n t^n = \left(1 - \frac{1}{2}t^2\sigma(t)\right)\Psi(t).$$

PROPOSITION 7.3. *For $n > 0$, equality holds in Proposition 7.1 if, and only if, $n - 1$ is a triangular number. In the case of equality, the leading term of $a(n, q) - 1$ is q^{-n} .*

PROOF: Using (7.23) and (6.6), we find that

$$(7.25) \quad a(n, q) - 1 = -\frac{\lambda_{n+1}}{q^n} - \frac{(\phi_{n+1} + \lambda_{n+2})}{q^{n+1}} + \dots$$

The Proposition now follows from (7.22). □

COROLLARY 7.4. *Propositions 7.1 and 7.3 remain true with $s_M(n, q) - s_M(\infty, q)$ in place of $a(n, q) - 1$.*

PROOF: By (3.6) and (6.5),

$$s_M(n, q) - s_M(\infty, q) = a(n, q)\omega(n, q) - \omega(\infty, q).$$

Using this and (7.25), we get

$$(7.26) \quad s_M(n, q) - s_M(\infty, q) = -\frac{\lambda_{n+1}}{q^n} - \frac{(\phi_{n+1} + \lambda_{n+2} - \lambda_{n+1} - 1)}{q^{n+1}} + \dots,$$

from which the result follows as before. □

In order to investigate the leading terms in (7.23), (7.25) and (7.26) more closely, we need to know the value of ϕ_n . Its determination is elementary but rather complicated. We shall therefore omit the detailed working and merely set down the final result. But before doing so we note a striking property of ϕ_n .

LEMMA 7.5. $\phi_n + \phi_{n+1} \in \{0, 1, -1\}$ for all $n > 0$.

PROOF: Although this can be deduced (with some labour) from the later tables, we shall give an independent proof. In view of (7.24), what the Lemma asserts is that the coefficient of t^n in the power series expansion of

$$(*) \quad (1+t) \left(1 - \frac{1}{2} t^2 \sigma(t) \right) \Psi(t) = \left(t + \frac{1-t^3}{1-t^4} \right) \Psi(t)$$

is 0, 1 or -1 whenever $n \geq 2$ (the series begins $1 + 2t + \dots$).

Now, the coefficient of t^n in $\left((1-t^3)/(1-t^4) \right) \Psi(t)$ is $v_n - w_n$, where v_n, w_n are the numbers of $T(m) \leq n$ and $\equiv n, n+1 \pmod{4}$ respectively. Suppose that

$$T(8r+s) \leq n < T(8r+s+1),$$

where $0 \leq s \leq 7$. If $r' < r$, then the values of $T(8r'), T(8r'+1), \dots, T(8r'+7)$ modulo 4 are 0, 1, 3, 2, 2, 3, 1, 0; these numbers therefore make no contribution to $v_n - w_n$. So we need only consider $T(8r), T(8r+1), \dots, T(8r+s)$. It is straightforward to check that, whatever the value of n modulo 4, these numbers contribute 0, 1 or -1 to $v_n - w_n$. For example, if $s = 5$ and $n \equiv 1 \pmod{4}$, then the contributions to v_n, w_n are respectively the numbers of 1's, 2's in the sequence 0, 1, 3, 2, 2, 3, so that $v_n - w_n = -1$.

The coefficient of t^n in the remaining part $t\Psi(t)$ of (*) is 1 if n has the form $1+T(m)$ and 0 otherwise. Thus, it remains only to check that, if $n = T(8r+s)+1 \geq 2$, then $v_n - w_n = 0$ or -1 . This is again straightforward, using the fact that $n < T(8r+s+1)$ (this is where the assumption that $n \geq 2$ comes in). For example, if $s = 4$, then $n \equiv 2+1 = 3 \pmod{4}$ and so $v_n - w_n$ is the number of 3's minus the number of 0's in the sequence 0, 1, 3, 2, 2, namely 0. □

In order to describe the value of ϕ_n , we write n in the form

$$(7.27) \quad n = T(8m+r) + 4b + i,$$

where

$$(7.28) \quad m \geq 0, 0 \leq r \leq 7, 0 \leq b, 0 \leq i \leq 3, 4b + i \leq 8m + r.$$

(The final condition in (7.28) ensures that $n < T(8m+r+1)$.) In the table of values of ϕ_n that follows, the 8 panels correspond to the values 0, \dots , 7 of r and the 4 rows in each panel (reading down from the top) to the values 0, 1, 2, 3 of i . When $b = i = 0$ (so that $n = T(8m+r)$) the value in the table has to be increased by 1: the emended

value is given in square brackets in the first row of each panel.

$ \begin{array}{l} -2(m-b) \quad [-2m+1] \\ (r=0) \quad 2(m-b) \\ -2(m-b) \\ 2(m-b)-1 \end{array} $	$ \begin{array}{l} -2m \quad [-2m+1] \\ (r=1) \quad 2m \\ -2m-1 \\ 2m+1 \end{array} $
$ \begin{array}{l} -2(m-b)-1 \quad [-2m] \\ (r=2) \quad 2(m-b)+1 \\ -2(m-b) \\ 2(m-b)-1 \end{array} $	$ \begin{array}{l} -2m-1 \quad [-2m] \\ (r=3) \quad 2m+1 \\ -2m-1 \\ 2m+1 \end{array} $
$ \begin{array}{l} -2(m-b)-1 \quad [-2m] \\ (r=4) \quad 2(m-b)+1 \\ -2(m-b)-1 \\ 2(m-b) \end{array} $	$ \begin{array}{l} -2m-1 \quad [-2m] \\ (r=5) \quad 2m+1 \\ -2m-2 \\ 2m+2 \end{array} $
$ \begin{array}{l} -2(m-b)-2 \quad [-2m-1] \\ (r=6) \quad 2(m-b)+2 \\ -2(m-b)-1 \\ 2(m-b) \end{array} $	$ \begin{array}{l} -2m-2 \quad [-2m-1] \\ (r=7) \quad 2m+2 \\ -2m-2 \\ 2m+2 \end{array} $

REMARKS.

- (1) For $n > 0$, if ϕ_n, ϕ_{n+1} are both nonzero, then they have opposite signs (the case $n = 0$ is exceptional as $\phi_0 = \phi_1 = 1$). This may be seen by inspection or directly from Lemma 7.5.
- (2) For fixed m and fixed *odd* r (but varying b, i), $|\phi_n|$ remains approximately constant at the value $2m$ (which is roughly $(n/8)^{1/2}$ since n is roughly $(8m)^2/2$). If $m > 0$, ϕ_n is never 0 or 1.
- (3) For fixed m and fixed *even* r , $|\phi_n|$ varies between approximately 0 and $2m$. Except in the one case $m = r = 0$, ϕ_n always assumes the values 0 and 1.

Our results yield the following detailed information about $a(n, q) - 1$. We have $a(0, q) - 1 = 0$ and now assume that $n > 0$.

If $n = T(\mu) + 1$, that is, $n = 1, 2, 4, 7, 11, 16, \dots$, then $a(n, q) - 1 = q^{-n} + \dots$. In all other cases, $\|a(n, q) - 1\|_q \leq q^{-(n+1)}$.

If $n = T(\mu)$ ($\mu > 1$), that is, if $n = 3, 6, 10, 15, \dots$, then $a(n, q) - 1 = (1 - \phi_{n+1})q^{-(n+1)} + \dots$ and $1 - \phi_{n+1}$ is nonzero except when $n = 3, 6, 10, 15$.

Finally, if n has neither of the forms above, then $a(n, q) - 1 = -\phi_{n+1}q^{-(n+1)} + \dots$ and ϕ_{n+1} is nonzero if, and only if, n has none of the following forms:

$$\begin{aligned}
 &5, 9, 14, \\
 &32m^2 + 40m + 12 \qquad (m \geq 0), \\
 &32m^2 + 56m + (23, 24 \text{ or } 25) \qquad (m \geq 0), \\
 &32m^2 + 8m + (-1, 0 \text{ or } 1) \qquad (m \geq 1), \\
 &32m^2 + 24m + 4 \qquad (m \geq 1).
 \end{aligned}$$

Corresponding results can be proved for the differences

$$a^+(n, q) - a^+(n - 1, q) = s_G(n, q) - s_G(n - 1, q)$$

and thence also for $s_G(n, q) - s_G(\infty, q)$ and $c_G(n, q) - c_G(n - 1, q)$ (see (3.5)). This can be done by applying the method used above to $(1 - t)P^+(q, t)$ or, as we shall do here, by referring back to the results for $(1 - t)P(q, t)$ using the simple relation (3.3). With the same kind of notation as before:

$$\begin{aligned}
 (1 - t)P^+(q, t) &= \mathcal{A}_-^+ + \sum_{r=0}^{\infty} \mathcal{A}_r^+, \\
 \mathcal{A}_-^+ &= q \sum_{n=0}^{\infty} \lambda_n^+ \left(\frac{t}{q}\right)^n, \\
 \mathcal{A}_0^+ &= \sum_{n=0}^{\infty} \phi_n^+ \left(\frac{t}{q}\right)^n,
 \end{aligned}$$

one finds that

$$\begin{aligned}
 \lambda_n &= \lambda_n^+ + \lambda_{n-1}^+, \\
 \phi_n &= \phi_n^+ + \phi_{n-1}^+ + \lambda_{n-1}^+,
 \end{aligned}$$

or, in solved form,

$$\begin{aligned}
 \sum \lambda_n^+ t^n &= (1 + t)^{-1} \left(\sum \lambda_n t^n \right), \\
 \sum \phi_n^+ t^n &= (1 + t)^{-1} \left(\sum \phi_n t^n \right) - \frac{t}{1 + t} \left(\sum \lambda_n^+ t^n \right).
 \end{aligned}$$

As before, we have

$$(7.29) \quad a^+(n, q) - a^+(n - 1, q) = \frac{\lambda_n^+}{q^{n-1}} + \frac{\phi_n^+}{q^n} + \dots ,$$

$$(7.30) \quad a^+(n, q) - 1 + q^{-1} = -\frac{\lambda_{n+1}^+}{q^n} - \frac{(\phi_{n+1}^+ + \lambda_{n+2}^+)}{q^{n+1}} + \dots .$$

The results that follow are set down without proof. The values of the λ_n^+ are a little more complicated than those of the λ_n in (7.22). We have

$$(7.31) \quad \lambda_0^+ = \lambda_1^+ = 0 .$$

Suppose now that $n \geq 2$ and let

$$T(m) + 1 \leq n < T(m + 1) + 2 \quad (m \geq 0) .$$

then

$$\lambda_m^+ = \begin{cases} 0 & (m \text{ odd}) , \\ (-1)^{k+1} & (m \text{ even}) , \end{cases}$$

where

$$k = n - T(m) - 2 .$$

PROPOSITION 7.6. *Equality holds in Proposition 7.2 if, and only if, $T(m) + 1 \leq m < T(m + 1) + 1$ for an even $m \geq 0$. In the case of equality, the leading term of $a^+(n, q) - 1 + q^{-1}$ is $\pm q^{-n}$.*

The final result may be compared with (3.19).

PROPOSITION 7.7. $\|c_G(n, q) - c_G(n - 1, q)\|_q \leq q^{-(2n-1)}$ with equality if, and only if, $T(m) + 2 \leq n < T(m + 1) + 2$ for an even $m \geq 0$.

REFERENCES

- [1] G.I. Lehrer, 'The cohomology of the regular semisimple variety', *J. Algebra* **199** (1998), 666-689.
- [2] G.I. Lehrer and G.B. Segal, 'Homology stability for classical regular semisimple varieties', (Report 98-27 (September 1998), School of Mathematics and Statistics, University of Sydney).
- [3] P.M. Neumann and C.E. Praeger, 'Cyclic matrices over finite fields', *J. London Math. Soc. (2)* **52** (1995), 263-284.

School of Mathematics and Statistics
 University of Sydney
 New South Wales 2006
 Australia