THE NUMBER OF MATRICES OVER A FINITE FIELD WITH PRESCRIBED EIGENSPACES

by Arne Dür

Let F be a finite field with q elements.
By a "partial partition" of F^m, I understand a set π of subspaces of F^m whose sum is direct. The type of π

$$\alpha = (1^{\alpha(1)}2^{\alpha(2)}..)$$

is defined by $\alpha(i)$ = number of blocks of π of F-dimension i . Let $A=\{\alpha=(1^{\alpha(1)}2^{\alpha(2)}..);\text{almost all } \alpha(i)=0\}$ denote the set of types. Then $gew(\alpha) := \Sigma_{i=1}^{\infty} i\alpha(i) = \dim_F(\Sigma_\pi V) \leq m$, and $|\alpha| := \Sigma_{i=1}^{\infty} \alpha(i)$ is the number of blocks of π .

In this article, we are concerned with the following counting problem:
Let π be an arbitrary partial partition of F^m. What is the number of m×m-matrices g with entries in F such that π is just the set of eigenspaces of g ?
Since this number depends only on m and on the type α of π, we denote it by $f_q(\alpha,m)$. Obviously $f_q(\alpha,m)=0$ if $|\alpha|>q$, because a matrix over F has at most q eigenspaces in F^m. The other values of f_q are given by their generating function.

<u>Theorem</u>: For any $\alpha=(1^{\alpha(1)}2^{\alpha(2)}..)\in A$ with $|\alpha|\leq q$ and $l:=gew(\alpha)$,

$$\Sigma_{n=0}^{\infty} f_q(\alpha,l+n)\frac{w^n}{b_q(n)} = \frac{q!}{(q-|\alpha|)!} \left(\Pi_{j=0}^{l}(1-q^j w)^{\gamma(j)} \right) e_q\left(-\frac{w}{q-1}\right)^{q-1} .$$

Here $b_q(n)=(q^n-1)(q^n-q)..(q^n-q^{n-1})$ is the order of the general linear group of F^m,
$\gamma(j)=q-1-\Sigma_{i=0}^{j}\alpha(l-i)$ for $j=0,1,..,l-1$ but $\gamma(l)=-1$, and
$e_q(z)=\Sigma_{k=0}^{\infty}\frac{z^k}{[k]!}$ is the q-exponential function (see [1],p.29)
($[k]!=[k][k-1]..[1]$, $[k]=(q^k-1)/(q-1)$). □

The main steps in the proof are

(i) to derive an explicit formula for the $f_q(\alpha,m)$ (which is improper to calculations) by Möbius inversion on the lattice of partial partitions of F^m

(ii) to calculate the generating function of the $f_q(\alpha,m)$ using the power series representation of the affine monoid of multiplicative functions

(compare [2],p.160,161).

In the sequel, I examine two special cases.

(1) π is empty, i.e. $\alpha=(1^0 2^0 ..)=0$:
In this case, $f_q(\alpha,m)$ is the number of $m\times m$-matrices over F having no eigenvalues in F. For brevity, set $z_q(m) := f_q(0,m)$.
Applying the theorem yields

$$\Sigma_{n=0}^{\infty} z_q(n)\frac{w^n}{b_q(n)} = e_q(-\frac{w}{q-1})^{q-1}/(1-w) \qquad (*) \quad .$$

A similar, but more complicated formula was obtained by J.P.S. Kung in [5],p.147, where a vector space analogue of the Pólya cycle index is introduced. From the relation (*) we get a recursion formula for the $z_q(m)$:

$z_q(0) = 1$ and

$$z_q(m+1) = q^{m+1}(q^m-1)z_q(m) - q^m\Sigma_{j=1}^{m}(-1)^j\binom{q}{j+1}\frac{b_q(m)}{b_q(m-j)}z_q(m-j) \quad .$$

For instance,

$$z_q(1) = 0$$
$$z_q(2) = \frac{1}{2}(q-1)^2q^2$$
$$z_q(3) = \frac{1}{3}(q-1)^3q^4(q+1)^2$$
$$z_q(4) = \frac{1}{8}(q-1)^4q^7(q^2+q+1)(3q^3+4q^2+5q+2) \quad .$$

By the recursion formula, we have the following result.

<u>Proposition</u>: $z_q(m)$ has the form $P_m(q)/m!$, where P_m is a polynomial in one variable X with integer coefficients. If $m\geq 2$, then P_m has the degree m^2, the divisor $(X-1)^m X^m$ and the leading coefficient

$$m!\ \Sigma_{i=0}^{m}\frac{(-1)^i}{i!} = r(m)$$

which is the m-th derangement number. In particular,

$$\lim_{q\to\infty} z_q(m)/q^{m^2} = r(m)/m! = \lim_{q\to\infty} \frac{z_q(m)}{q-1} \Big/ \frac{b_q(m)}{q-1} \quad . \qquad \square$$

Observe that $z_q(m)/q^{m^2}$, $r(m)/m!$ and $\frac{z_q(m)}{q-1}/\frac{b_q(m)}{q-1}$ can be interpreted as the probabilities that a m×m-matrix over F has no eigenvalues in F, that a permutation of m elements leaves no element fixed resp. that a projektive transformation in the projective space of F^m has no fixed point.

If q=2, then $z_2(m)/b_2(m)=\Sigma_{j=0}^{m} \frac{(-1)^j}{[j]!}$. The numbers

$$D_n(q) = [n]! \ \Sigma_{j=0}^{n} \frac{(-1)^j}{[j]!}$$

have been studied by A.M. Garsia and J. Remmel in [3] as a q-analogue of the derangement numbers r(n). For arbitrary q however, $z_q(m)/b_q(m) \neq D_m(q)/[m]!$ in general, e.g. when q=3 and m=2.

Finally, it can be shown that, as $q\to 1$, $z_q(m)/b_q(m)$ tends to the coefficient of w^m in the power series $\exp(-\Sigma_{k=1}^{\infty} w^k/k^2)/(1-w)$. Since $\Sigma_{m=1}^{\infty} \frac{r(m)}{m!} w^m = \exp(-w)/(1-w)$, we conclude that in general $z_q(m)/b_q(m)$ doesn't converge to $r(m)/m!$ when $q\to 1$.

(2) π has only one block V which is of dimension $l\geq 1$, i.e. $\alpha=(1^0 \ldots l-1^0 l^1 l+1^0 \ldots)=\varepsilon(l)$:

In this case, $f_q(\alpha,m)$ is the number of linear transformations g in F^m whose only eigenspace is V. If g has the unique eigenvalue $\lambda\in F$, then $g-\lambda id$ has the unique eigenvalue $0\in F$ and vice versa. Hence $n_q(l,m) := f_q(\varepsilon(l),m)/q$ counts the linear transformations in F^m with kernel V having no non-zero eigenvalue in F. Using $(1-w)(1-qw)\ldots(1-q^{l-1}w)e_q(-\frac{w}{q-1}) = e_q(-\frac{q^l w}{q-1})$, we infer from the theorem that

$$\Sigma_{n=0}^{\infty} n_q(l,l+n)\frac{w^n}{b_q(n)} = \frac{e_q(-\frac{q^l w}{q-1})^{q-1}}{(1-w)(1-qw)\ldots(1-q^l w)} \quad .$$

References:

[1] Cigler J.,Elementare q-Identitäten,Publ.IRMA,Strasbourg(1982), 23-57.

[2] Dür A.,Kombinatorische Strukturen,Unipotente Gruppen und Potenzreihen-Darstellungen,Publ.IRMA,Strasbourg(1984),133-161.

[3] Garsia A.M.-J.Remmel,A Combinatorial Interpretation of q-Derangement and q-Laguerre Numbers,Europ.J.Combinatorics (1980) 1,47-59.

[4] Goldman J.-G.C.Rota,Finite Vector Spaces and Eulerian Generating Functions,Studies in Appl.Math.49(1970),239-258.

[5] Kung J.P.S.,The Cycle Structure of a Linear Transformation over a Finite Field,Lin.Alg. and Its Appl.36:141-155(1981).

Arne Dür
Department of Mathematics
University of Innsbruck
6020 Innsbruck, Innrain 52, Austria