ILLINOIS JOURNAL OF MATHEMATICS
Volume 32, Number 2, Summer 1988

PRODUCTS OF MATRICES OVER A FINITE FIELD

BY

AMOS KOVACS

1. Introduction

Let F_q be a finite field of q elements. Let $\mathscr{C}$ be a class of $n \times n$ matrices over F_q. Now, choosing l $n \times n$ matrices $A_l, \ldots, A_1$ we ask: what is the probability that the product $A_l \ldots A_1$ will belong to $\mathscr{C}$? We considered this question in an earlier paper [5], where $\mathscr{C}$ was the class of matrices of rank r (and nullity $t = n - r$). To introduce the results of [5] we need some notation:

$$[n] = (q^n - 1)[n-1] = (q^n - 1)(q^{n-1} - 1)\ldots(q-1), \qquad [0] = 1, \tag{1}$$

$$[n|k] = \frac{[n]}{[n-k]} = (q^n - 1)(q^{n-1} - 1)\ldots(q^{n-k+1} - 1), \qquad n \geq k \geq 0, \tag{2}$$

$$\begin{bmatrix} n \\ k \end{bmatrix} = \frac{[n]}{[k][n-k]} = \frac{(q^n - 1)\ldots(q^{n-k+1} - 1)}{(q^k - 1)\ldots(q-1)}, \qquad n \geq k \geq 0. \tag{3}$$

The $\begin{bmatrix} n \\ k \end{bmatrix}$'s are called the Gaussian coefficients and give the number of k-dimensional subspaces of an n space over F_q (for more details see [4]).

In [5] we proved that the probability for a product of k $n \times n$ matrices to be of rank $r = n - t$ is

$$^k p_{nn-t} = \left(q^{-n^2 k}\right)\left(^k m_{nn-t}\right) \tag{4}$$

where

$$^k m_{nn-t} = q^{\frac{1}{2}(n-1)(nk-2t)+\binom{t}{2}} \begin{bmatrix} n \\ t \end{bmatrix} \sum_{\sigma=0}^{t} (-1)^{t-\sigma} \begin{bmatrix} t \\ \sigma \end{bmatrix} q^{\binom{\sigma}{2}} \times \left(q^{\binom{\sigma+1}{2}} [n|n-\sigma]\right)^k. \tag{5}$$

Received July 17, 1986.

In particular, the probability for the product of k matrices to be zero is

$$ {}^{k}p_{n0} = q^{-\binom{n+1}{2}k-\binom{n}{2}} \sum_{\sigma=0}^{n} (-1)^{n-\sigma} q^{\binom{\sigma}{2}} \begin{bmatrix} n \\ \sigma \end{bmatrix} \left(q^{\binom{\sigma+1}{2}} [n|n-\sigma] \right)^{k}. \quad (6) $$

In a further paper [6] we utilized the results of [5] to answer the basic question for 2 classes, nilpotent matrices and idempotent matrices.

In the present paper we generalize the methods of [6] and show how they can be used for any class of matrices $\mathscr{C}$ which is invariant under inner-automorphisms, provided we know the number of matrices from $\mathscr{C}$ in right (left) ideals of the ring of $n \times n$ matrices over F_q (Lemma 1).

After proving the basic counting lemma, we proceed to give some applications. In Sections 3 and 4 we treat two easy cases: matrices of given trace and matrices of given determinant. Next, in Section 5, we turn to matrices of given characteristic polynomial and in Section 6 to diagonalizable matrices. The results of these two sections generalize the results of [6]. Clearly the method yields itself to many more applications.

Apart from the notation introduced in (1)–(6) we shall use the following notation throughout the paper.

Let N be a fixed n-dimensional space over F_q and $\mathfrak{R} = \mathrm{Hom}_F(N, N) = M_n(F_q)$ where matrices will be viewed as linear transformations on N when convenient.

The number of elements in a finite set S is denoted by $\sharp S$. Thus

$$ \sharp N = q^n, \quad \sharp \mathfrak{R} = q^{n^2}. \quad (7) $$

If $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_t)$ is a vector of integers with $\alpha_1 + \alpha_2 + \cdots + \alpha_t \leq n$ we define

$$ \begin{bmatrix} n \\ \alpha \end{bmatrix} = \frac{[n]}{[\alpha_1][\alpha_2] \cdots [\alpha_t][n - \alpha_1 - \alpha_2 - \cdots - \alpha_t]}. \quad (8) $$

We shall also use the abbreviation

$$ \langle \alpha \rangle = \sum_{i \neq j} \alpha_i \alpha_j. \quad (9) $$

2. The basic counting lemma

Let $\mathscr{C}$ be a class of matrices in $\mathfrak{R} = M_n(F_q)$ which is invariant under inner automorphisms, i.e., $A\mathscr{C}A^{-1} = \mathscr{C}$ for all invertible $A \in \mathfrak{R}$. Now let e_{ij} be the standard matrix units of $\mathfrak{R}$ and $e_r = e_{11} + e_{22} + \cdots + e_{rr}$. Let us now denote by c_r the number of matrices in $\mathscr{C}$ whose $n - r$ last columns are zero, i.e.,

$$ c_r = \sharp \mathscr{C} \cap \mathfrak{R} e_r. \quad (10) $$

Note that by the invariance of $\mathscr{C}$ we could have defined c_r as $\#\mathscr{C} \cap \mathfrak{R}B$ where B is any matrix of rank r in $\mathfrak{R}$. Let us now denote by $\gamma(l, n, q)$ the probability that the product of l matrices chosen at random from $\mathfrak{R}$ will fall into $\mathscr{C}$.

$$\gamma(l, n, q) = \mathscr{P}\{A_l \dots A_1 \in \mathscr{C}\}. \tag{11}$$

Our basic lemma expresses $\gamma(l, n, q)$ in terms of the c_r and the probabilities that a product of k matrices will have rank r—which have been computed in [5].

LEMMA 1.

$$\gamma(l, n, q) = q^{-n^2 l} \sum_{t=0}^{n} q^{nt} c_{n-t}{}^{l-1} m_{nn-t} \tag{12}$$

where

$$\begin{aligned} {}^k m_{nn-t} = q^{\frac{1}{2}(n-1)(nk-2t)+\binom{t}{2}} \begin{bmatrix} n \\ t \end{bmatrix} \sum_{\sigma=0}^{t} (-1)^{t-\sigma} \begin{bmatrix} t \\ \sigma \end{bmatrix} q^{\binom{\sigma}{2}} \\ \times \left(q^{\binom{\sigma+1}{2}} [n|n-\sigma] \right)^k. \end{aligned} \tag{13}$$

Proof. For $l = k + 1 \geq 1$ we have

$$\begin{aligned} \gamma(k+1, n, q) &= \mathscr{P}\{A_{k+1} \dots A_1 \in \mathscr{C}\} \\ &= \sum_{r=0}^{n} \mathscr{P}\{A_{k+1}B \in \mathscr{C} | \text{rank } B = r\} \mathscr{P}\{\text{rank } A_k \dots A_1 = r\}. \end{aligned} \tag{14}$$

Now,

$$\begin{aligned} &\mathscr{P}\{A_{k+1}B \in \mathscr{C} | \text{rank } B = r\} \\ &\quad = q^{-n^2} \#\{A | AB \in \mathscr{C}, \text{rank } B = r\} \\ &\quad = q^{-n^2} \#\{A | AB = 0, \text{rank } B = r\} \#\{\mathfrak{R}B \cap \mathscr{C}\} \\ &\quad = q^{-n^2} q^{n(n-r)} c_r \\ &\quad = q^{-nr} c_r. \end{aligned}$$

On the other hand, from [5, Theorem 2] we know that

$$\mathscr{P}\{\text{rank}(A_k \dots A_1) = r\} = q^{-n^2 k}\, {}^k m_{nr}$$

where ${}^k m_{nr}$ is given by (13).

Combining these into (14) and changing the index of summation from r to $t = n - r$ will yield the result.

In the upcoming sections we shall exhibit several applications of the basic counting lemma, starting with some very simple ones and going on to greater complexity. Some more applications may be found in [6].

3. Fixed trace

Let λ be any element in F_q and $\mathscr{C}$ the set of all matrices in $\mathfrak{R}$ of trace λ. Clearly $\mathscr{C}$ has q^{n^2-1} elements and almost as clearly

$$c_r = \#\mathscr{C} \cap \mathfrak{R}e_r = q^{r^2-1}q^{r(n-r)} = q^{rn-1},\ r \geq 1,$$
$$c_0 = \delta_{\lambda 0}. \tag{15}$$

Let us now confine ourselves for a minute to the case $\lambda = 0$. Then, if we denote by $\gamma_\lambda(k+1, n, q)$ the probability that the product of $k+1$ $n \times n$ matrices will have trace zero, we have by (15) and (12),

$$\begin{aligned}
\gamma_0(k+1, q, n) &= q^{-n^2(k+1)} \sum_{t=0}^{n} q^{nt} c_{n-t}\, {}^k m_{nn-t} \\
&= q^{-n^2(k+1)} \left(\sum_{t=0}^{n-1} q^{nt} q^{(n-t)n-1}\, {}^k m_{nn-t} + q^{n^2}\, {}^k m_{n0} \right) \\
&= q^{-n^2(k+1)+n^2-1} \left(\sum_{t=0}^{n-1} {}^k m_{nn-t} + q\, {}^k m_{n0} \right) \\
&= q^{-n^2k-1} \left(\sum_{t=0}^{n} {}^k m_{nn-t} + (q-1)\, {}^k m_{n0} \right).
\end{aligned}$$

Now, $\sum_{t=0}^{n} {}^k m_{nn-t}$ is, by the definition of ${}^k m_{nn-t}$, just the count of all k-tuples of $n \times n$ matrices, hence it equals q^{n^2k}; therefore

$$\gamma_0(k+1, q, n) = q^{-1}\left(1 + q^{-n^2k}(q-1)\left({}^k m_{n0}\right)\right) = q^{-1}\left(1 + (q-1)\left({}^k p_{n0}\right)\right)$$

where ${}^k p_{n0}$ is the probability that the product of k $n \times n$ matrices is zero and is given by (6).

Now, if $\lambda \neq 0$ we can proceed in the same way using $c_0 = 0$ or we may use symmetry to conclude that $(q-1)\gamma_\lambda(k+1, q, n) + \gamma_0(k+1, q, n) = 1$.

This proves:

THEOREM 1. *The probability that the product of l $n \times n$ matrices over a field of q elements will have trace λ is*

$$\begin{aligned}
&q^{-1}\left(1 + (q-1)\left({}^{l-1} p_{n0}\right)\right) && \text{if } \lambda = 0, \\
&q^{-1}\left(1 - \left({}^{l-1} p_{n0}\right)\right) && \text{if } \lambda \neq 0,
\end{aligned} \tag{16}$$

where ${}^{k}p_{n0}$ *is the probability of the product k matrices to be zero and is given by* (6).

4. Fixed determinant

We shall now determine the probability for the product $A_1 \dots A_l$ to have a given determinant. Again let d be any element of F_q, and $\mathscr{C}^d$ the set of matrices of determinant d in $\mathfrak{R}$. Applying the well known formula for the number of regular matrices in $\mathfrak{R}$ we get

$$c_n^0 = \sharp \mathscr{C}^0 = q^{n^2} - q^{\binom{n}{2}}[n] = q^{\binom{n}{2}}\left(q^{\binom{n+1}{2}} - [n]\right), \tag{17}$$

while for $r < n$ we have

$$c_r^0 = \sharp \mathscr{C}^0 \cap \mathfrak{R}e_r = \sharp \mathfrak{R}e_r = q^{n(n-r)}. \tag{18}$$

This takes care of matrices of determinant 0. As for matrices of determinant $d \neq 0$ clearly their number is independent of d and so

$$c_n^d = \sharp \mathscr{C}^d = c_n^1 = \sharp \mathscr{C}^1 = \frac{q^{\binom{n}{2}}[n]}{q-1} = q^{\binom{n}{2}}[n|n-1], \tag{19}$$

while for $r < n$,

$$c_r^d = c_r^1 = 0. \tag{20}$$

Now, if $\gamma_1(k+1, n, q)$ will denote the probability that the product of $k+1$ matrices will have determinant 1, we have by (12)

$$\gamma_1(k+1, q, n) = q^{-n^2(k+1)} \sum_{t=0}^{n} q^{nt} c_{n-t}\, {}^{k}m_{nn-t} = q^{-n^2(k+1)} q^{\binom{n}{2}} [n|n-1]\, {}^{k}m_{nn}.$$

Now, by (5),

$${}^{k}m_{nn} = q^{\binom{n}{2}k}[n|n]^k$$

and so

$$\gamma_1(k+1, q, n) = \frac{q^{-n^2(k+1)} q^{\binom{n}{2}(k+1)} [n]^{k+1}}{q-1} = \frac{\left(q^{-\binom{n+1}{2}}[n]\right)^{k+1}}{q-1}.$$

Now $\gamma_0(k+1, q, n)$ can be computed directly using (17) and (18), or by using symmetry we once again have $\gamma_0 + (q-1)\gamma_1 = 1$. This proves:

THEOREM 2. *The probability that the product of l $n \times n$ matrices over a field of q elements will have determinant λ is*

$$\begin{cases} \dfrac{F(q,n)^l}{q-1} & \text{for } \lambda \neq 0, \\ 1 - F(q,n)^l & \text{for } \lambda = 0, \end{cases} \tag{21}$$

where

$$F(q,n) = q^{-\binom{n+1}{2}}[n]. \tag{22}$$

Buckheister in [2] computed the number of matrices in $\mathfrak{R}$ with given trace and rank. As a further application of the basic counting lemma one could use that result to calculate the probability that a product of l matrices will have given trace and rank. We turn now to applications concerned with the minimal and characteristic polynomial of the product.

5. Fixed characteristic polynomial

We now compute the probability that the product $A_1 \dots A_l$ will have a given characteristic polynomial. We shall use a result of Gerstenhaber [3] who computed the number of matrices in $\mathfrak{R}$ having a given characteristic polynomial. As previously noted we shall use the notation introduced in [3]:

$$F(q,r) = q^{-\binom{r+1}{2}}[r].$$

Let $f(x) = f_1^{m_1}(x) f_2^{m_2}(x) \dots f_d^{m_d}(x)$ a polynomial of degree n in $F_q[x]$ with $f_i(x)$ irreducible of degree d_i, $\Sigma d_i m_i = n$. Let $\mathscr{C}$ be the class of all matrices in $\mathfrak{R}$ having $f(x)$ as characteristic polynomial. It is proved in [3] that

$$c_n^f = \sharp\mathscr{C} = q^{n^2-n} \frac{F(q,n)}{\prod F(q^{d_i}, m_i)}. \tag{23}$$

Note that the result holds for $m_i = 0$ since $F(q^{d_i}, 0) = 1$.

We shall now want to compute c_r^f, the number of matrices having $f(x)$ as characteristic polynomial in $\mathfrak{R}e_r$.

To that purpose, let us rewrite $f(x)$ as

$$f(x) = x^{m_0} f_1^{m_1}(x) \cdots f_d^{m_d}(x)$$

where $x \neq f_i(x)$ and $m_0 \geq 0$. Now, any matrix T in $\mathfrak{R}e_r$ may be written in block form as

$$T = \left(\begin{array}{c|c} \hat{T} & 0 \\ \hline \hat{T}_1 & 0 \end{array}\right)$$

where $\hat{T}$ is r by r and $\hat{T}_1$ is $n - r$ by r. If $\chi_T(x)$ denotes the characteristic polynomial of T, we have $\chi_T(x) = x^{n-r}\chi_{\hat{T}}(x)$; hence we conclude

$$c_r^f = \begin{cases} 0 & \text{if } r < n - m_0, \\ q^{r(n-r)}c_r^{f/x^{n-r}} & \text{if } r \geq n - m_0. \end{cases} \tag{24}$$

Therefore, if we denote by $c_f(k+1, n, q)$ the probability that the product of $k+1$ matrices will have $f(x)$ as characteristic polynomial, we have from (24) and (12):

$$\begin{aligned} c_f(k+1, n, q) &= q^{-n^2(k+1)} \sum_{t=0}^{n} q^{nt} c_{n-t}^f {}^k m_{nn-t} \\ &= q^{-n^2(k+1)} \sum_{t=0}^{m_0} q^{nt} q^{(n-t)t} q^{(n-t)^2-(n-t)} \\ &\quad \times \frac{F(q, n-t)}{F(q, m_0 - t)\prod F(q^{d_i}, m_i)} {}^k m_{nn-t}. \end{aligned}$$

Substituting in the expression for ${}^k m_{nn-t}$ and abbreviating $\prod_{i=1}^{d} (q^{d_i}, m_i)$ by P^{-1} we get, after some routine simplifications,

$$c_f(k+1, n, q) = Pq^{-\binom{n+1}{2}(k+1)-n} \sum_{\sigma=0}^{m_0} q^{\binom{\sigma}{2}} \left(q^{\binom{\sigma+1}{2}} [n|n-\sigma]\right)^k p_\sigma(q) \tag{25}$$

where

$$p_\sigma(q) = q^{m_0}\begin{bmatrix} n \\ \sigma \end{bmatrix}[n-\sigma|n-m_0] \sum_{t=\sigma}^{m_0} (-1)^{t-\sigma} q^{\binom{m_0-t}{2}+t} \begin{bmatrix} m_0 - \sigma \\ m_0 - t \end{bmatrix}.$$

Substituting $t - \sigma = \nu$ and $m_0 - \sigma = \pi$ we get

$$p_\sigma(q) = q^{m_0+\sigma}\begin{bmatrix} n \\ \sigma \end{bmatrix}[n-\sigma|n-m_0] \sum_{\nu=0}^{\pi} (-1)^\nu q^{\binom{\pi-\nu}{2}+\nu} \begin{bmatrix} \pi \\ \pi - \nu \end{bmatrix}. \tag{26}$$

Considering now the inner summation in (26), we can replace $\left[\begin{smallmatrix}\pi\\ \pi-\nu\end{smallmatrix}\right]$ by $\left[\begin{smallmatrix}\pi\\ \nu\end{smallmatrix}\right]$ and using Lemma 2 of [6] we have

$$\sum_{\nu=0}^{\pi}(-1)^{\nu}q^{\binom{\pi-\nu}{2}+\nu}\left[\begin{smallmatrix}\pi\\ \nu\end{smallmatrix}\right]=\delta_{\pi 0}+\delta_{\pi 1}(1-q).$$

Substituting this in (26), and (26) in turn back in (25), proves:

THEOREM 3. *Let* $f(x)=x^{m_0}f_1^{m_1}(x)f_2^{m_2}(x)\dots f_d^{m_d}(x)$ *be a polynomial in* $F_q[x]$ *where the* $f_i(x)\neq x$ *are different irreducible polynomials of degree* d_i *and* $m_i\geq 0$. *The probability that the product of* l $n\times n$ *matrices over* F_q *will have* $f(x)$ *as characteristic polynomial is*

$$\frac{q^{\left(\binom{m_0+1}{2}-\binom{n+1}{2}\right)l+(m_0-n)}}{\prod_{i=1}^{d}F(q^{d_i},m_i)}[n|n-m_0]^l\left(1-\left(\frac{q^{m_0}-1}{q^{m_0}}\right)^l\right)\tag{27}$$

where

$$F(q,n)=q^{-\binom{n+1}{2}}[n].$$

Remark. If we consider $f(x)=x^n$ the theorem will give the probability for the product $A_l\dots A_1$ to be nilpotent. In this case $n=m_0$ while $m_i=0$ for $i\geq 1$. Then (27) collapses to

$$1-\left(\frac{q^n-1}{q^n}\right)^l$$

which is just Theorem 1 of [6].

6. Diagonalizable matrices

As a final application of the basic counting lemma we are going to address the question of diagonalizable matrices over F_q. The methods of this section, after some simple alterations could also handle matrices with given minimal polynomial with distinct roots.

A matrix T in $\mathfrak{N}$ is diagonalizable in $\mathfrak{N}$ if and only if its minimal polynomial $m(x)$ splits into distinct linear factors over F_q,

$$m(x)=(x-\lambda_1)\dots(x-\lambda_t)$$

where $\lambda_i\neq\lambda_j$, which is equivalent to N's being a direct sum

$$N=N_1\oplus\cdots\oplus N_t$$

where the N_i are the eigenspaces of T belonging to λ_i.

Recall that a composition of n into t parts is a vector of positive integers

$$\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_t)$$

where $\Sigma\alpha_i = n$. We denote by $C(n, t)$ the set of all compositions of n into t parts.

In Lemma 7 of [2] we have calculated the number of decompositions of N into 2 parts. An easy generalization of it will yield:

LEMMA 2. *The number of decompositions of N into a direct sum*

$$N = N_1 \oplus N_2 \oplus \cdots \oplus N_t$$

is

$$\sum_{\alpha \in C(n,t)} q^{\Sigma_{i \neq j} \alpha_i \alpha_j} \begin{bmatrix} n \\ \alpha \end{bmatrix}. \tag{28}$$

By the discussion above, (28) is also the number of matrices in $\mathfrak{R}$ with minimal polynomial having exactly t distinct linear factors. Finally, counting all the possibilities for the set of eigenvalues $\{\lambda_1, \ldots, \lambda_t\}$ and summing up over t will give:

LEMMA 3. *The number of diagonalizable matrices in $\mathfrak{R}$ is*

$$\sum_{t=1}^{q} \begin{pmatrix} q \\ t \end{pmatrix} \sum_{\alpha \in C(n,t)} q^{\Sigma_{i \neq j} \alpha_i \alpha_j} \begin{bmatrix} n \\ \alpha \end{bmatrix}. \tag{29}$$

The same result, albeit in a slightly different form and with a more involved argument may be found in Theorem 2 of [1].

To facilitate notation, we shall denote the sum $\Sigma_{i \neq j} \alpha_i \alpha_j$ for a vector α by $\langle \alpha \rangle$.

Having counted the number of diagonalizable matrices in $\mathfrak{R}$ we easily calculate their number $c_r = \sharp \mathscr{C} \cap \mathfrak{R}B$ in any left ideal $\mathfrak{R}B$ of $\mathfrak{R}$, where $\mathscr{C}$ of course is just the set of diagonalizable matrices.

LEMMA 4. *Let B be a matrix of rank r; then the number of diagonalizable matrices in $\mathfrak{R}B$ is*

$$c_r = \sum_{s=1}^{q-1} \begin{pmatrix} q-1 \\ s \end{pmatrix} \sum_{j=s}^{r} q^{j(n-j)} \begin{bmatrix} r \\ j \end{bmatrix} \sum_{\alpha \in C(j,s)} q^{\langle \alpha \rangle} \begin{bmatrix} s \\ \alpha \end{bmatrix}, \quad r \geq 1,$$

$$c_0 = 1. \tag{30}$$

Proof. T is in $\mathfrak{R}B$ and is diagonalizable if and only if $N = \operatorname{Ker} T \oplus T(N)$ with $\operatorname{Ker} B \subseteq \operatorname{Ker} T$ and $T|_{T(N)}$ is diagonalizable and regular. If T is of rank

j, we must have $j \leq r$ and we may choose $\operatorname{Ker} T$ to contain $\operatorname{Ker} B$ in

$$\begin{bmatrix} n-(n-r) \\ n-(n-j) \end{bmatrix} = \begin{bmatrix} r \\ j \end{bmatrix}$$

ways.

Now we choose the image $T(N)$ to complement $\operatorname{Ker} T$; there are $q^{j(n-j)}$ ways to do that. Next we decide on the number s of nonzero eigenvalues for T and choose the eigenvalues $\lambda_1 \dots \lambda_s$; this can be done in $\binom{q-1}{s}$ ways. Note that $s \leq q-1$ and $s \leq j$. Finally we have to decide on the decomposition of $T(N)$ into s eigenspaces—by Lemma 2 this can be done in

$$\sum_{\alpha \in C(j,s)} q^{\langle \alpha \rangle} \begin{bmatrix} j \\ \alpha \end{bmatrix}$$

ways.

Multiplying all the factors and summing up over all possible numbers of nonzero eigenvalues $s = 1 \dots q-1$ and over all possible ranks for T, $j = s \dots r$ we get the total number of matrices in $\mathscr{C} \cap \mathfrak{R}B$.

Note that (30) does not hold for $r = 0$ but $c_0 = 1$.

Now, letting $\gamma(k+1, n, q)$ be the probability that the product of $k+1$ matrices will be diagonalizable, by (12) we have

$$\begin{aligned} \gamma(k+1, n, q) &= q^{-n^2(k+1)} \sum_{t=0}^{n} q^{nt} c_{n-t}\, {}^k m_{nn-t} \\ &= q^{-n^2(k+1)} \sum_{t=0}^{n-1} q^{nt} c_{n-t}\, {}^k m_{nn-t} + q^{-n^2 k}\, {}^k m_{nn}. \end{aligned} \tag{31}$$

In order to evaluate the first term of (31), note that we may as well sum for $t = 0, \dots, n$ since for $t = n$, (30) yields zero. Using this and introducing another abbreviation,

$$\begin{aligned} A^n_{\sigma,s} &= A^{m+\sigma}_{\sigma,s}(q) \\ &= \sum_{i=0}^{m} \sum_{j=s}^{m-i} \left((-1)^i q^{\binom{i+1}{2} + i\sigma + j(n-j)} \begin{bmatrix} m \\ i, j \end{bmatrix} \sum_{\alpha \in C(j,s)} q^{\langle \alpha \rangle} \begin{bmatrix} s \\ \alpha \end{bmatrix} \right). \end{aligned} \tag{32}$$

After some simple manipulations, we get:

THEOREM 4. *The probability that the product of l $n \times n$ matrices over a field of q elements will be diagonalizable over the field is*

$${}^k p_{nn} + q^{-\binom{n+1}{2} l - \binom{n}{2}} \sum_{\sigma=0}^{n} \frac{q^{\binom{\sigma}{2}}}{[n-\sigma]} \left(q^{\binom{\sigma+1}{2}} [n \mid n-\sigma] \right)^l \sum_{s=1}^{q-1} \binom{q-1}{s} A^n_{\sigma,s}(q), \tag{33}$$

where $A^n_{\sigma,s}(q)$ are given by (32) *and ${}^kp_{nn}$ is the probability that the product of k matrices will be zero and is given by* (6).

References

1. J.V. Brawley and G.L. Mullen, *A note of equivalence classes of matrices over a finite field*, Internat. J. Math., Math. Sci., vol. 4 (1981), pp. 279–287.
2. P.G. Buckhiester, *The number of $n \times n$ matrices of rank r and trace α over a finite field*, Duke Math. J., vol. 39 (1972), pp. 695–699.
3. M. Gerstenhaber, *On the number of nilpotent matrices with coefficients in a finite field*, Illinois J. Math., vol. 5 (1961), pp. 330–333.
4. I.P. Goulden and D.M. Jackson, *Combinatorial enumeration*, Wiley, New York, 1983.
5. A. Kovacs, *On the probability that the product of k $n \times n$ matrices over a finite field will be zero*, J. Combin. Theory Ser. A, vol. 45 (1987), pp. 290–299.
6. _____, *Some enumeration problems for matrices over a finite field*, Linear Algebra Appl., vol. 94 (1987), pp. 223–236.
7. I. Reiner, *On the number of matrices with given characteristic polynomial*, Illinois J. Math., vol. 5 (1961), pp. 324–329.

The University of Texas at Austin
Austin, Texas

Center for Military Analyses (17), P.O. Box 2250
Haifa, Israel