JOURNAL OF COMBINATORIAL THEORY, Series A 53, 157–160 (1990)

Note

A Combinatorial Construction for Products of Linear Transformations over a Finite Field

I. P. GOULDEN AND D. M. JACKSON

Department of Combinatorics and Optimization, University of Waterloo, Waterloo, Ontario, Canada N2L 3G1

Communicated by the Managing Editors

Received December 2, 1987

Kovacs (*J. Combin. Theory, Ser. A* **45** (1987), 290–299) has derived an expression for the number of ordered k-tuples, $(A_k, ..., A_1)$, of $n \times n$ matrices over $GF(q)$ whose product $A_k \cdots A_1$ has prescribed rank. We give a combinatorial construction for this result. © 1990 Academic Press, Inc.

Let $\mathscr{V}$ be a vector space of dimension n over $GF(q)$. We determine the number, $p_k(n, i, j)$, of k-tuples of linear operators over $\mathscr{V}$ such that the rank of the restriction of their product to a prescribed i-dimensional subspace of $\mathscr{V}$ is equal to j.

The set of all linear operators on $\mathscr{V}$ is denoted by $\mathscr{H}$. If $T = (T_k, ..., T_1) \in \mathscr{H}^k$, then we denote $T_k \cdots T_1 \in \mathscr{H}$ by $\hat{T}$. Throughout, $\dim_{GF(q)}$ and $\text{span}_{GF(q)}$ are abbreviated to dim and span. The set of all i-dimensional subspaces of $\mathscr{V}$ is denoted by $\binom{\mathscr{V}}{i}$. Implicit use is made of the fact that, if $\mathscr{V}_1, \mathscr{V}_2$ are vector spaces, then $\mathscr{V}_1 \cong \mathscr{V}_2$ if and only if $\dim \mathscr{V}_1 = \dim \mathscr{V}_2$, so enumerative quantities associated with vector spaces depend only on dimensions (and, of course, the ground field). It is well known (see, for example, [1, 2]) that $|\binom{\mathscr{V}}{i}| = \prod_{k=1}^{i} (1 - q^{n-k+1})/(1 - q^k)$, the *Gaussian coefficient*, which is denoted by $\binom{n}{i}_q$.

We begin with a combinatorial derivation of a linear relationship involving $p_k(n, i, j)$.

THEOREM 1. *For* $0 \leqslant l \leqslant i \leqslant n$,

$$\sum_{j=l}^{i} p_k(n, i, j)\, q^{l(i-j)} \binom{j}{l}_q = \binom{i}{l}_q p_k(n, l, l).$$

0097-3165/90 $3.00

Proof. Let $\mathscr{U} \in \binom{\mathscr{V}}{i}$ be arbitrary but fixed. We derive two different expressions for ψ, the cardinality of the set $\{(\mathscr{X}, T) \in \binom{\mathscr{U}}{l} \times \mathscr{H}^k : r(\hat{T}|_{\mathscr{X}}) = l\}$.

First, by summing over $\mathscr{X}$ we see that $\psi = \sum_{\mathscr{X} \in \binom{\mathscr{U}}{l}} |\{T \in \mathscr{H}^k : r(\hat{T}|_{\mathscr{X}}) = l\}| = |\binom{\mathscr{U}}{l}| \cdot |\{T \in \mathscr{H}^k : r(\hat{T}|_{\mathscr{X}_0}) = l\}|$, where $\mathscr{X}_0 \in \binom{\mathscr{U}}{l}$ is arbitrary but fixed. Thus

$$\psi = \binom{i}{l}_q p_k(n, l, l). \tag{1}$$

Second, by summing over T, we see that $\psi = \sum_{j=l}^{i} \sum_{T \in \mathscr{H}^k} |\{\mathscr{X} \in \binom{\mathscr{U}}{l} : r(\hat{T}|_{\mathscr{X}}) = l,\ r(\hat{T}|_{\mathscr{U}}) = j\}|$. We now give a construction for $\mathscr{X}$. Given T, let $\mathscr{A}_{\hat{T}} \in \binom{\mathscr{U}}{j}$ be arbitrary but fixed such that $\ker \hat{T}|_{\mathscr{U}} \oplus \mathscr{A}_{\hat{T}} = \mathscr{U}$ where $\dim \mathscr{A}_{\hat{T}} = j$. Thus $r(\hat{T}|_{\mathscr{U}}) = j$. Let $\mathscr{Y} \in \binom{\mathscr{A}_{\hat{T}}}{l}$ have a canonical ordered basis $(y_1, ..., y_l)$, and let $c_1, ..., c_l \in (\ker \hat{T}|_{\mathscr{U}})^l$. Then

(i) $\operatorname{span}(y_1 + c_1, ..., y_l + c_l) \in \binom{\mathscr{U}}{l}$,

(ii) $\hat{T} \operatorname{span}(y_1 + c_1, ..., y_l + c_l) = \hat{T}\mathscr{Y}$ so $r(\hat{T}|_{\operatorname{span}(y_1 + c_1, ..., y_l + c_l)}) = r(\hat{T}|_{\mathscr{Y}}) = l$,

(iii) $\operatorname{span}(y_1 + c_1, ..., y_l + c_l) = \operatorname{span}(y_1 + d_1, ..., y_l + d_l)$ if and only if $c_m = d_m$ for $m = 1, ..., l$.

We may therefore suppose that $\mathscr{X} = \operatorname{span}(y_1 + c_1, ..., y_l + c_l)$ for some $(y_1, ..., y_l)$ and $(c_1, ..., c_l)$, so $|\{\mathscr{X} \in \binom{\mathscr{U}}{l} : r(\hat{T}|_{\mathscr{X}}) = l,\ r(\hat{T}|_{\mathscr{U}}) = j\}| = \sum_{\mathscr{Y} \in \binom{\mathscr{A}_{\hat{T}}}{l}} |(\ker \hat{T}|_{\mathscr{U}})|^l = \sum_{\mathscr{Y} \in \binom{\mathscr{A}_{\hat{T}}}{l}} q^{(i-j)l} = \binom{j}{l}_q q^{(i-j)l}$. Thus

$$\begin{aligned} \psi &= \sum_{j=l}^{i} \binom{j}{l}_q q^{(i-j)l} |\{T \in \mathscr{H}^k : r(\hat{T}|_{\mathscr{U}} = j\}| \\ &= \sum_{j=l}^{i} \binom{j}{l}_q q^{(i-j)l} p_k(n, i, j). \end{aligned} \tag{2}$$

The result follows by equating (1) and (2). ∎

To evaluate $p_k(n, i, j)$ explicitly, we invert the linear relationship given in Theorem 1, and evaluate $p_k(n, l, l)$, for $0 \leqslant l \leqslant n$, using the next two propositions.

PROPOSITION 2. *Let $f_0, f_1, ..., g_0, g_1, ...$ be formal Laurent series in the indeterminate u. Then*

$$f_j = \sum_{l \geqslant j} \binom{l}{j}_u g_l \qquad \textit{for} \quad j = 0, 1, ...$$

if and only if

$$g_l = \sum_{j \geqslant l} (-1)^{j-l} u^{\binom{j-l}{2}} \binom{j}{l}_u f_j \qquad \textit{for} \quad l = 0, 1, ...$$

Proof. Let $j!_u$ denote $(1-u)(1-u^2)\cdots(1-u^j)$. The zeta and Möbius functions for the lattice of partitions ordered by refinement (Goldman and Rota [1]) are, respectively, $\zeta(t)=\sum_{k\geqslant 0} t^k/k!_u$ and $\mu(t)=\sum_{k\geqslant 0}(-1)^k u^{\binom{k}{2}} t^k/k!_u$ and, moreover, $\zeta(t)\,\mu(t)=1$. Let $f(t)=\sum_{k\geqslant 0} f_k t^k\, k!_u$ and $g(t)=\sum_{k\geqslant 0} g_k t^k\, k!_u$. Then $f(t)=\zeta(t^{-1})\, g(t)$ if and only if $g(t)=\mu(t^{-1})\, f(t)$, and the result follows by comparing the coefficients in each of these. ∎

PROPOSITION 3. *For* $0\leqslant l\leqslant n$,

$$p_k(n, l, l)=\{q^{n(n-l)}(q^n-1)(q^n-q)\cdots(q^n-q^{l-1})\}^k.$$

Proof. $p_k(n, l, l)=|\{T\in \mathscr{H}^k: r(\hat{T}|_{\mathscr{X}})=l\}|$, where $\mathscr{X}\in\binom{\mathscr{V}}{l}$ is arbitrary but fixed. Thus $r(T_s|_{\mathscr{X}})=l$ for $s=1, ..., k$ so $p_k(n, l, l)=p_1^k(n, l, l)$. But $p_1(n, l, l)=q^{n(n-l)}(q^n-1)(q^n-q)\cdots(q^n-q^{l-1})$, since the basis elements of $\mathscr{X}$ must be mapped into a linearly independent l-tuple of elements of $\mathscr{V}$, of which there are clearly $(q^n-1)(q^n-q)\cdots(q^n-q^{l-1})$. The remaining $n-l$ elements in the basis of $\mathscr{V}$ formed by extending the basis of $\mathscr{X}$ can be mapped to any of the q^n elements of $\mathscr{V}$. ∎

We now complete the evaluation of $p_k(n, i, j)$.

COROLLARY 4. *For* $0\leqslant j\leqslant i\leqslant n$,

$$p_k(n, i, j)=\frac{1}{q^{\binom{i}{2}-\binom{j}{2}}}\binom{i}{j}_q \sum_{l=j}^{i}\binom{i-j}{l-j}_q (-1)^{l-j} q^{\binom{i-l}{2}} \times \{q^{n(n-l)}(q^n-1)(q^n-q)\cdots(q^n-q^{l-1})\}^k.$$

Proof. Multiplying both sides of Theorem 1 by $(-1)^l q^{\binom{l+1}{2}-li}$, we obtain

$$\sum_{j\geqslant l} p_k(n, i, j)\, q^{-\binom{j}{2}}(-1)^j(-1)^{j-l}\, q^{\binom{j-l}{2}}\binom{j}{l}_q = (-1)^l\, q^{\binom{l+1}{2}-li}\binom{i}{l}_q p_k(n, l, l).$$

Now let $g_l=(-1)^l\, q^{\binom{l+1}{2}-li}\binom{i}{l}_q\, p_k(n, l, l)$ and $f_j=p_k(n, i, j)\, q^{-\binom{j}{2}}(-1)^j$ and the result follows from Proposition 2, after substituting the value for $p_k(n, l, l)$ given by Proposition 3. ∎

Kovacs' [3] expression for the number of ordered k-tuples of matrices over $GF(q)$ whose product has rank t is obtained by setting $i=n$, $j=n-t$ in Corollary 4.

Algebraic proofs of Theorem 1 and Corollary 4 can be obtained as follows. Let $M_k = [p_k(n, i, j)]_{0 \leqslant i,j \leqslant n}$, $Q = [\binom{i}{j}_q / q^{j(i-j)}]_{0 \leqslant i,j \leqslant n}$, and $D_k = \mathrm{diag}(p_k(n, 0, 0), ..., p_k(n, n, n))$. The following facts can be verified: $M_1 Q = QD_1$, $M_k = M_1^k$, and $D_k = D_1^k$. Such a Q exists because M_1 is diagonalizable, since its eigenvalues, $p_1(n, i, i)$, for $i = 0, ..., n$, are mutually distinct. These results may be combined to give $M_k Q = QD_k$, and thence Theorem 1 by comparing the (i, l)-elements of these matrices. Corollary 4 follows by using the fact that $M_k = QD_k Q^{-1}$, where $Q^{-1} = [(-1)^{i-j} \binom{i}{j}_q / q^{\binom{i}{2} - \binom{j}{2}}]_{0 \leqslant i,j \leqslant n}$.

Acknowledgments

This work was supported by Grants A8907 and A8235 from the Natural Sciences and Engineering Research Council of Canada.

References

1. J. R. Goldman and G.-C. Rota, On the foundations of combinatorial theory IV: Finite vector spaces and Eulerian generating functions, *Stud. Appl. Math.* **49** (1970), 239–258.
2. I. P. Goulden and D. M. Jackson, "Combinatorial Enumeration," Wiley, New York, 1983.
3. 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* **45** (1987), 290–299.