JOURNAL OF COMBINATORIAL THEORY, Series A 37, 80–84 (1984)

Note

Bijective Methods in the Theory of Finite Vector Spaces*

ALBERT NIJENHUIS,[†] ANITA E. SOLOW,[‡] AND HERBERT S. WILF[†]

[†]*Department of Mathematics, University of Pennsylvania, Philadelphia, Pennsylvania 19104;*
and [‡]*Department of Mathematics, Grinnell College, Grinnell, Iowa 50112*

Communicated by the Managing Editors

Received April 26, 1982

1. INTRODUCTION

Combinatorial properties of vector spaces over finite fields have been extensively investigated (see Goldman and Rota [1, 2], Knuth [3], Milne [4], Calabi and Wilf [5], etc.). In this paper we will obtain a number of results by a unified method. The method, as used in [5], is the observation that the canonical invariant of a vector subspace over a finite field is a matrix over the field, in reduced row echelon form (rref), whose rows span the subspace. If two such matrices differ in even a single entry then they represent different vector subspaces.

Combinatorially this means that to count subspaces we just count matrices in rref. Here are the results we obtain in this way:

(a) a "one-line" pictorial proof of an elegant description, due to Pólya [6], of the coefficients of the Gaussian polynomials in terms of areas of certain lattice walks (Section 2, below).

(b) a bijective proof of a three term recurrence relation satisfied by the "Galois coefficients" that was found by Goldman and Rota [1] by formal methods.

(c) an evaluation of the alternating sum of the Gaussian coefficients.

First recall that a $k \times n$ matrix over a field of q elements is in rref if in each row $i = 1,..., k$ the first nonzero entry is a 1, the index of the column in which the 1 occurs ("pivotal column") strictly increases with i, and the k pivotal columns are, in order, the columns of the $k \times k$ identity matrix.

* Research supported by the National Science Foundation.

0097-3165/84 $3.00

Since we will never need to do field arithmetic, we will assume that the entries of the marix are from the set $Q = \{0, 1, \ldots, q-1\}$ of "letters," and q need not be a prime power. The Gaussian coefficient

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \frac{(q^n - 1)(q^{n-1} - 1) \cdots (q^{n-k+1} - 1)}{(q^k - 1)(q^{k-1} - 1) \cdots (q - 1)} \tag{1}$$

counts the $k \times n$ matrices in rref over Q (see below). The bijections that we will produce will be mappings between certain sets of matrices over Q in rref.

2. Pólya's Theorem on Lattice Walks

Let $p(n, k, r)$ be the coefficients in the expansion

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \sum_r p(n, k, r)\, q^r. \tag{2}$$

Then we have

THEOREM 1(Pólya, 1969). *$p(n, k, r)$ is the number of walks on lattice points in the first quadrant that begin at $(0,k)$, move at each stage either a unit to the right or down, end at $(n-k, 0)$, and have "area" r, i.e., r unit cells lie between the walk and the lines $y = k$ and $x = n - k$.*

The one-line proof that we promised is the one jagged line in Fig. 1. There we show a given $k \times n$ matrix in rref, in which the k pivotal columns are to be ignored, leaving a $k \times (n-k)$ array. The jagged line starts at the top left corner of the matrix, exactly encloses the entries that are allowed to be different from 0 or 1, and ends at the lower right corner.

If the area above the jagged line is r, then each of those r entries might hold any of the q elements of Q, and so there are exactly q^r matrices over Q in rref that yield the same walk. Hence the number of $k \times n$ matrices over Q that are in rref is given by the polynomial on the right hand side of (2). Since

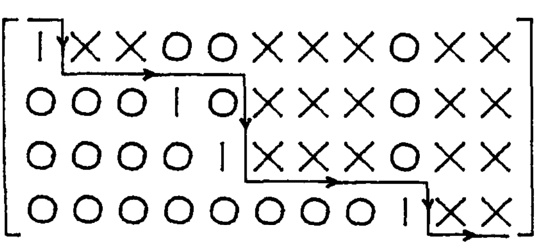

FIGURE 1

this number equals the number of k dimensional vector subspaces of n-space over $GF(q)$, Eq. (2) holds when q is a prime power, and so, since both sides are polynomials, it holds identically in q. This proof is similar in spirit to the one in [3], though it is a bit more general in that it gives information even when q is not a prime power.

3. Bijective Mappings

Let $RR(n, k)$ $(0 \leqslant k \leqslant n)$ be the set of $k \times n$ matrices over Q in rref, let $RR(n)$ be the union $\bigcup_k RR(n, k)$, and finally let $G_n = |RR(n)|$. We will now give a bijective proof of the following result of [1].

THEOREM 2. *The Galois numbers G_n satisfy the recurrence*

$$G_{n+1} = 2G_n + (q^n - 1)\, G_{n-1} \qquad (n \geqslant 0;\ G_{-1} = 0;\ G_0 = 1). \tag{3}$$

(Of course, when q is a prime power, (3) is a recurrence for the number of subspaces of n-space.)

For the proof, we define three injection mappings:

$$\alpha_n: RR(n, k) \to RR(n+1, k),$$

$$\beta_n: RR(n, k) \to RR(n+1, k+1),$$

$$\gamma_n: RR(n-1, k) \times Q^n \to RR(n+1, k+1),$$

where

$\alpha_n(W)$ has a first column of zeros, followed by the columns of W,

$\beta_n(W)$ borders W with a new last row and last column, all zeros except a 1 in the last row and last column,

$\gamma_n(W, \mathbf{u})$ borders W with a new first column, a new first row, and a new last column. The new leading element is 1, below it are all zeros, and to the right of it zeros are placed above the pivotal columns of W. The remaining n places, in the first row and last column, are filled with the entries of $\mathbf{u}$, in order.

LEMMA 1. *The images of the three maps*

$$\alpha_n, \qquad \beta_n|(RR(n) - \alpha_{n-1}RR(n-1)), \qquad \textit{and} \quad \gamma_n$$

are disjoint subsets of $RR(n+1)$.

Proof. The matrices in $\mathrm{Im}(\alpha_n)$ have a first column of zeros. The matrices in $RR(n) - \alpha_{n-1}RR(n-1)$ have as first column a pivotal column (= column 1 of the identity matrix), and their images under β_n have the same property. The matrices in $\mathrm{Im}(\gamma_n)$ also have a pivotal column for a first column. The last column of a matrix of the image of $RR(n) - \alpha_{n-1} RR(n-1)$ under β_n is also a pivotal column (= the last column of the identity matrix), while the last pivot column of a matrix in $\mathrm{Im}(\gamma_n)$ occurs before the last column, completing the proof of the lemma.

LEMMA 2. *Every matrix in $RR(n+1)$ is either in the image of α_n, of $\beta_n|(RR(n) - \alpha_{n-1}RR(n-1))$, or of γ_n.*

Proof. Let *FP* (resp. *LP*) be the proposition that the first (resp. last) column of the matrix is pivotal. The three cases in the statement of the lemma are respectively, $\sim FP$, $FP \wedge LP$, $FP \wedge (\sim LP)$.

Proof of Theorem 2. Since the mappings are injective and the three images partition $RR(n+1)$, we have

$$\begin{aligned} G_{n+1} &= |RR(n+1)| = |\alpha_n RR(n)| + |\beta_n(RR(n) - \alpha_{n-1}RR(n-1))| \\ &\quad + |\gamma_n(RR(n-1) \times Q^n)| \\ &= |RR(n)| + |RR(n) - \alpha_{n-1}RR(n-1)| + |RR(n-1) \times Q^n| \\ &= G_n + (G_n - G_{n-1}) + q^n G_{n-1} \\ &= 2G_n + (q^n - 1)\, G_{n-1}. \end{aligned}$$

Remark 1. A slight modification of the argument would have produced a bijection between $RR(n+1) \cup RR(n-1)$ and

$$RR(n) \dot{\cup} RR(n) \dot{\cup} RR(n-1) \times Q^n$$

giving an even "purer" proof of (3). The above proof was chosen, however, because it more clearly reveals the recursive structure of $RR(n)$.

Remark 2. The argument actually proves more, namely, it is a bijective proof of the recurrence

$$\begin{bmatrix} n+1 \\ k \end{bmatrix}_q = \begin{bmatrix} n \\ k \end{bmatrix}_q + \begin{bmatrix} n \\ k-1 \end{bmatrix}_q + (q^n - 1)\begin{bmatrix} n-1 \\ k-1 \end{bmatrix}_q \tag{4}$$

from which (3) follows by summation on k.

Finally, suppose we define

$$F_n(x) = \sum_k \begin{bmatrix} n \\ k \end{bmatrix}_q x^k. \tag{5}$$

Then (4) gives

$$\begin{gathered} F_{n+1}(x) = (1+x)\, F_n(x) + (q^n - 1)\, xF_{n-1}(x) \\ (n \geqslant 0;\ F_{-1} = 0;\ F_0 = 1). \end{gathered} \tag{6}$$

If we now put $x = -1$ we obtain immediately Gauss' evaluation of the alternating sum

$$\sum_k (-1)^k \begin{bmatrix} n \\ k \end{bmatrix}_q = (1 - q^{n-1})(1 - q^{n-3}) \cdots (1 - q) \qquad n \text{ even}$$

$$= 0 \qquad n \text{ odd.}$$

References

1. J. Goldman and G.-C. Rota, The number of subspaces of a vector space, *in* "Recent Progress in Combinatorics" (W. Tutte Ed.), pp. 75–84, Academic Press, New York, 1969.
2. J. Goldman and G.-C. Rota, On the foundations of combinatorial theory. IV. Finite vector spaces and Eulerian generating functions, *in* "Studies in Applied Mathematics," Vol. XLIX, No. 3, 1970.
3. D. Knuth, Subspaces, subsets and partitions, *J. Combin. Theory* **10** (1971), 178–180.
4. S. C. Milne, Mappings of subspaces into subsets, preprint.
5. E. Calabi and H. S. Wilf, On the sequential and random selection of subspaces over a finite field, *J. Combin. Theory* **22** (1977), 107–109.
6. G. Pólya, Gaussian binomial coefficients and the enumeration of inversions, *in* "Proceedings, 2nd Chapel Hill Conference on Combinatorial Mathematics and Its Applications, August 1970," pp. 381–384, Univ. of North Carolina, Chapel Hill, 1970.