Integer Sequences and Matrices Over Finite Fields

Kent E. Morrison
Department of Mathematics
California Polytechnic State University
San Luis Obispo, CA 93407

kmorriso@calpoly.edu

February 1, 2006

Abstract

In this expository article we collect the integer sequences that count several different types of matrices over finite fields and provide references to the Online Encyclopedia of Integer Sequences (OEIS). Section 1 contains the sequences, their generating functions, and examples. Section 2 contains the proofs of the formulas for the coefficients and the generating functions of those sequences if the proofs are not easily available in the literature. The cycle index for matrices is an essential ingredient in most of the derivations.

2000 Mathematics Subject Classification: Primary 05A15, 15A33; Secondary 05A10, 05A30, 11B65, 11B73.

Keywords: Integer sequences, Matrices over finite fields, Cycle index for matrices.

Notation

q	a prime power
$\mathbf{F}_q$	field with q elements
$\mathrm{GL}_n(q)$	group of $n \times n$ invertible matrices over $\mathbf{F}_q$
$\mathrm{M}_n(q)$	algebra of $n \times n$ matrices over $\mathbf{F}_q$
$\gamma_n(q)$	order of the group $\mathrm{GL}_n(q)$
γ_n	order of $\mathrm{GL}_n(q)$ with q understood
ν_d	number of irreducible monic polynomials of degree d over $\mathbf{F}_q$

Sequences	**Section**	**OEIS**
All matrices	1.1	A002416
Invertible matrices	1.2	A002884
Subspaces, q-binomial coefficients	1.3	A022166–188
		A006116–122
		A015195–217
Splittings (direct sum decompositions)	1.4	
q-Stirling numbers, q-Bell numbers	1.4	
Flags of subspaces	1.5	A005329, A069777
Linear binary codes	1.6	A022166, A076831
Matrices by rank	1.7	
Linear derangements	1.8, 2.2	A002820
Projective derangements	1.8, 2.2	
Diagonalizable matrices	1.9, 2.3	
Projections	1.10, 2.4	A053846
Solutions of $A^k = I$	1.11, 2.5	A053718, 722, 725
		A053770–777
		A053846–849
		A053851–857
		A053859–863
Nilpotent matrices	1.12	A053763
Cyclic(regular) matrices	1.13, 2.6	
Semi-simple matrices	1.14, 2.7	
Separable matrices	1.15, 2.8	
Conjugacy classes	1.16, 2.9	A070933, A082877

1 The Sequences

References to the OEIS are accurate as of February 1, 2006. Sequences mentioned in this article may have been added since then and entries in the OEIS may have been modified.

1.1 $n \times n$ matrices over $\mathbf{F}_q$

Over the field $\mathbf{F}_q$ the number of $n \times n$ matrices is q^{n^2}. For $q = 2$ this sequence is A002416 of the OEIS, indexed from $n = 0$. The terms for $0 \le n \le 4$ are

$$1, 2, 16, 512, 65536.$$

1.2 Invertible matrices

The number of invertible $n \times n$ matrices is given by

$$\gamma_n(q) := |\mathrm{GL}_n(q)| = (q^n - 1)(q^n - q)(q^n - q^2) \cdots (q^n - q^{n-1}).$$

We will use γ_n in place of $\gamma_n(q)$ unless there is a need to be explicit about the base field. It is convenient to define γ_0 to be 1. For $q = 2$ the sequence is A002884, and from γ_0 to γ_5 the terms are

$$1, 1, 6, 168, 20160, 9999360.$$

A second formula for γ_n is

$$\gamma_n = (q-1)^n q^{\binom{n}{2}} [n]_q!,$$

where $[n]_q! := [n]_q[n-1]_q \cdots [2]_q[1]_q$ and $[i]_q := 1 + q + q^2 + \cdots + q^{i-1}$ are the q-analogs of $n!$ and i. Also, $[i]_q$ is the number of points in the projective space of dimension $i-1$ over $\mathbf{F}_q$.

A third formula is

$$\gamma_n = (-1)^n q^{\binom{n}{2}} (q;q)_n,$$

where $(a;q)_n$ is defined for $n > 0$ by

$$(a;q)_n := \prod_{j=0}^{n-1} (1 - aq^j).$$

Construct a random $n \times n$ matrix over $\mathbf{F}_q$ by choosing the entries independently and uniformly from $\mathbf{F}_q$. Then γ_n / q^{n^2} is the probability that the matrix is invertible, and this probability has a limit as $n \to \infty$

$$\lim_{n\to\infty} \frac{\gamma_n}{q^{n^2}} = \prod_{r \geq 1} \left(1 - \frac{1}{q^r}\right).$$

For $q = 2$ the limit is $0.28878\ldots$. For $q = 3$ the limit is $0.56012\ldots$. As $q \to \infty$ the probability of being invertible goes to 1.

1.3 Subspaces

The number of k-dimensional subspaces of a vector space of dimension n over $\mathbf{F}_q$ is given by the Gaussian binomial coefficient (also called the q-binomial coefficient)

$$\binom{n}{k}_q = \frac{(q^n - 1)(q^n - q)(q^n - q^2) \cdots (q^n - q^{k-1})}{(q^k - 1)(q^k - q)(q^k - q^2) \cdots (q^k - q^{k-1})}.$$

Also, we define $\binom{0}{0}_q = 1$. Other useful expressions for the Gaussian binomial coefficients are

$$\binom{n}{k}_q = \frac{[n]_q!}{[k]_q![n-k]_q!},$$

which shows the q-analog nature of the Gaussian coefficients, and

$$\binom{n}{k}_q = \frac{\gamma_n}{\gamma_k \gamma_{n-k} q^{k(n-k)}},$$

which comes from the transitive action of $\mathrm{GL}_n(q)$ on the set of subspaces of dimension k, the denominator being the order of the subgroup stabilizing one of the subspaces.

Entries A022166–A022188 are the triangles of Gaussian binomial coefficients for $q = 2$ to $q = 24$. Note that when q is not a prime power the formula does not count subspaces. For $q = 2$ the rows from $n = 0$ to 6 are

1						
1	1					
1	3	1				
1	7	7	1			
1	15	35	15	1		
1	31	155	155	31	1	
1	63	651	1395	651	63	1

For the Gaussian binomial coefficients we have the q-**binomial theorem** [2]

$$\prod_{1 \le i \le n} (1 + q^i t) = \sum_{0 \le k \le n} q^{\binom{k}{2}} \binom{n}{k}_q t^k.$$

Summing over k from 0 to n for a fixed n gives the total number of subspaces. Sequences A006116–A006122 and A015195–A015217 correspond to the values $q = 2, \ldots, 8$ and $q = 9, \ldots, 24$. (Same warning applies to those q that are not prime powers.) For $q = 2$ and $n = 0, \ldots, 8$ the sequence begins

$$1, 2, 5, 16, 67, 374, 2825, 29212, 417199.$$

1.4 Splittings

Let $\left\{ {n \atop k} \right\}_q$ be the number of direct sum splittings of an n-dimensional vector space into k non-trivial subspaces without regard to the order among the subspaces. These numbers are q-analogs of the Stirling numbers of the second kind, which count the number of partitions of an n-set into k non-empty subsets, and the notation follows that of Knuth for the Stirling numbers. Then it is easy to see that

$$\left\{ {n \atop k} \right\}_q = \frac{1}{k!} \sum_{\substack{n_1 + \cdots + n_k = n \\ n_i \ge 1}} \frac{\gamma_n}{\gamma_{n_1} \cdots \gamma_{n_k}}.$$

It is not difficult to verify that the triangle $\left\{ {n \atop k} \right\}_q$ satisfies the two variable generating function identity

$$1 + \sum_{n \ge 1} \sum_{k=1}^{n} \left\{ {n \atop k} \right\}_q \frac{u^n}{\gamma_n} t^k = \exp\left(t \sum_{r \ge 1} \frac{u^r}{\gamma_r} \right).$$

For $q = 2$ the entries for $1 \le n \le 6$ and $1 \le k \le n$ are

1					
1	3				
1	28	28			
1	400	1680	840		
1	10416	168640	277760	83328	
1	525792	36053248	159989760	139991040	27998208

Let b_n be the total number of non-trivial splittings of an n-dimensional vector space:

$$b_n = \sum_{k=1}^{n} \left\{ {n \atop k} \right\}_q .$$

The b_n are analogs of the Bell numbers counting the number of partitions of finite sets. Then we have the formula for the generating function for the b_n,

$$1 + \sum_{n\geq 1} b_n \frac{u^n}{\gamma_n} = \exp\left(\sum_{r\geq 1} \frac{u^r}{\gamma_r} \right).$$

For $q = 2$ the values of b_n for $n = 1, \ldots, 6$ are

$$1, 4, 57, 2921, 540145, 364558049.$$

Bender and Goldman [1] first wrote down the generating function for the q-Bell numbers, which, along with the q-Stirling numbers, can be put into the context of q-exponential families [10].

1.5 Flags

A **flag** of length k in a vector space V is an increasing sequence of subspaces

$$\{0\} = V_0 \subset V_1 \subset V_2 \subset \cdots V_k = V.$$

If $\dim V = n$, then a **complete flag** is a flag of length n. Necessarily, $\dim V_i = i$.

The number of complete flags of an n-dimensional vector space over $\mathbf{F}_q$ is

$$\binom{n}{1}_q \binom{n-1}{1}_q \cdots \binom{1}{1}_q = [n]_q [n-1]_q \cdots [1]_q = [n]_q!.$$

The reason is that having selected $V_1, \ldots, V_i$, the number of choices for V_{i+1} is $\binom{n-i}{1}_q$. Alternatively, the general linear group acts transitively on the set of complete flags. The stabilizer subgroup of the standard flag is the subgroup of upper triangular matrices, whose order is $(q-1)^n q^{\binom{n}{2}}$. Hence, the number of complete flags is

$$\frac{\gamma_n}{(q-1)^n q^{\binom{n}{k}}} = [n]_q!.$$

Define $[0]_q! = 1$. The sequence $[n]_q!$ for $q = 2$ is A005329. The terms for $n = 0, 1, 2, \ldots, 8$ are

$$1, 1, 3, 21, 315, 9765, 615195, 78129765, 19923090075.$$

By looking up the phrase "q-factorial numbers" in the OEIS one can find the sequences $[n]_q!$ for $q \leq 13$. The triangle of q-factorial numbers is A069777.

The q-multinomial coefficient

$$\binom{n}{n_1\ n_2\ \cdots\ n_k}_q := \frac{[n]_q!}{[n_1]_q! [n_2]_q! \cdots [n_k]_q!},$$

where $n = n_1 + \cdots + n_k$, is the number of flags of length k in an n-dimensional space such that $\dim V_i = n_1 + \cdots + n_i$.

1.6 Linear binary codes

An $[n, k]$ linear binary code is a k-dimensional subspace of the space of $\mathbf{F}_2^n$. Thus, the number of $[n, k]$ linear binary codes is the Gaussian binomial coefficient $\binom{n}{k}_2$ from section 1.3 and is given by the triangle A022166.

Two linear binary codes are **equivalent** (or isometric) if there is a permutation matrix P mapping one subspace to the other. The number of equivalence classes of $[n, k]$ codes is given by the triangle A076831. The early entries are identical with the corresponding binomial coefficients, but that does not hold in general. The rows for $n = 0$ to 6 are

1						
1	1					
1	2	1				
1	3	3	1			
1	4	6	4	1		
1	5	10	10	5	1	
1	6	16	22	16	6	1

For linear codes over other finite fields, the notion of equivalence uses matrices P having exactly one non-zero entry in each row and column. These matrices, as linear maps, preserve the Hamming distance between vectors. They form a group isomorphic to the wreath product of the multiplicative group of $\mathbf{F}_q$ with S_n.

There are more than a dozen sequences and triangles associated to linear binary codes in the OEIS. They are listed in the short index of the OEIS under "Codes."

1.7 Matrices by rank

The number of $m \times n$ matrices of rank k over $\mathbf{F}_q$ is

$$\begin{aligned}
&\binom{m}{k}_q (q^n - 1)(q^n - q)\cdots(q^n - q^{k-1}) \\
&= \binom{n}{k}_q (q^m - 1)(q^m - q)\cdots(q^m - q^{k-1}) \\
&= \frac{(q^m - 1)(q^m - q)\cdots(q^m - q^{k-1})\ \ (q^n - 1)(q^n - q)\cdots(q^n - q^{k-1})}{(q^k - 1)(q^k - q)\cdots(q^k - q^{k-1})}.
\end{aligned}$$

(To justify the first line of the formula note that the number of k-dimensional subspaces of $\mathbf{F}_q^m$ to serve as the column space of a rank k matrix is $\binom{m}{k}_q$. Identify the column space with the image of the associated linear map from $\mathbf{F}_q^n$ to $\mathbf{F}_q^m$. There are $(q^n - 1)(q^n - q)\cdots(q^n - q^{k-1})$ surjective linear maps from $\mathbf{F}_q^n$ to that k-dimensional image. The second line follows by transposing.)

Define the triangle $r(n, k)$ to be the number of $n \times n$ matrices of rank k over $\mathbf{F}_q$ and $r(0, 0) := 1$. Thus,

$$r(n, k) = \frac{\big((q^n - 1)(q^n - q)\cdots(q^n - q^{k-1})\big)^2}{(q^k - 1)(q^k - q)\cdots(q^k - q^{k-1})}.$$

For $q = 2$ the entries from $r(0,0)$ to $r(5,5)$ are

1					
1	1				
1	9	6			
1	49	294	168		
1	225	7350	37800	20160	
1	961	144150	4036200	19373760	9999360

1.8 Linear and projective derangements

A matrix is a **linear derangement** if it is invertible and does not fix any non-zero vector. Such a matrix is characterized as not having 0 or 1 as an eigenvalue. Let e_n be the number of linear derangements and define $e_0 = 1$. Then e_n satisfies the recursion

$$e_n = e_{n-1}(q^n - 1)q^{n-1} + (-1)^n q^{n(n-1)/2}.$$

For $q = 2$, the sequence is A002820 (with offset 2) and the first few terms beginning with e_0 are $1, 0, 2, 48, 5824, 2887680, \ldots$. The sequence can be obtained from the generating function

$$1 + \sum_{n\geq 1} \frac{e_n}{\gamma_n} u^n = \frac{1}{1-u} \prod_{r\geq 1} \left(1 - \frac{u}{q^r}\right).$$

The proof of this is in section 2. The asymptotic probability that an invertible matrix is a linear derangement is

$$\lim_{n\to\infty} \frac{e_n}{\gamma_n} = \prod_{r\geq 1} \left(1 - \frac{1}{q^r}\right).$$

The asymptotic probability that a square matrix is a linear derangement is

$$\lim_{n\to\infty} \frac{e_n}{q^{n^2}} = \prod_{r\geq 1} \left(1 - \frac{1}{q^r}\right)^2$$

A matrix over $\mathbf{F}_q$ is a **projective derangement** if the induced map on projective space has no fixed points. Equivalently, this means that the matrix has no eigenvalues in $\mathbf{F}_q$. If d_n is the number of such $n \times n$ matrices, then

$$1 + \sum_{n\geq 1} \frac{d_n}{\gamma_n} u^n = \frac{1}{1-u} \prod_{r\geq 1} \left(1 - \frac{u}{q^r}\right)^{q-1}.$$

For $q = 2$ the notions of projective and linear derangement are the same, and the corresponding sequence is given above. For $q = 3$ the sequence has initial terms from $n = 1$ to 5

$$0, 18, 3456, 7619508, 149200289280.$$

Since two matrices that differ by a scalar multiple induce the same map on projective space, the number of maps that are projective derangements is $d_n/(q-1)$. The asymptotic probability that a random invertible matrix is a projective derangement is the limit

$$\lim_{n\to\infty} \frac{d_n}{\gamma_n} = \prod_{r\geq 1} \left(1 - \frac{1}{q^r}\right)^{q-1}.$$

The asymptotic probability that a random $n \times n$ matrix is a projective derangement is

$$\lim_{n\to\infty} \frac{d_n}{q^{n^2}} = \prod_{r\geq 1} \left(1 - \frac{1}{q^r}\right)^{q}.$$

As $q \to \infty$, this probability goes to $1/e$, the same value as the asymptotic probability that a random permutation is a derangement.

1.9 Diagonalizable matrices

In this section let d_n be the number of diagonalizable $n \times n$ matrices over $\mathbf{F}_q$. Then

$$1 + \sum_{n\geq 1} \frac{d_n}{\gamma_n} u^n = \left(\sum_{m\geq 0} \frac{u^m}{\gamma_m} \right)^q.$$

It follows that

$$d_n = \sum_{n_1+\cdots+n_q=n} \frac{\gamma_n}{\gamma_{n_1}\cdots\gamma_{n_q}}.$$

For $q = 2$ this simplifies to

$$d_n = \sum_{i=0}^{n} \frac{\gamma_n}{\gamma_i \gamma_{n-i}}.$$

The sequence for d_1 to d_8 is

$$2, 8, 58, 802, 20834, 1051586, 102233986, 196144424834.$$

For $q = 3$ the five initial terms are

$$3, 39, 2109, 417153, 346720179.$$

For arbitrary q, we can easily find d_2,

$$\begin{aligned} d_2 &= \sum_{n_1+\cdots+n_q=2} \frac{\gamma_n}{\gamma_{n_1}\cdots\gamma_{n_q}} \\ &= q\frac{\gamma_2}{\gamma_0\gamma_2} + \binom{q}{2}\frac{\gamma_2}{\gamma_1\gamma_1} \\ &= \frac{q^4 - q^2 + 2q}{2}. \end{aligned}$$

1.10 Projections

A **projection** is a matrix P such that $P^2 = P$. Let p_n be the number of $n \times n$ projections. Then

$$1 + \sum_{n \geq 1} \frac{p_n}{\gamma_n} u^n = \left(\sum_{m \geq 0} \frac{u^m}{\gamma_m} \right)^2 .$$

It follows that

$$p_n = \sum_{0 \leq i \leq n} \frac{\gamma_n}{\gamma_i \gamma_{n-i}}.$$

In the sum the term $\gamma_n/\gamma_i\gamma_{n-i}$ is the number of projections of rank i. Projections are also characterized as diagonalizable matrices having eigenvalues 0 or 1. Thus, for $q = 2$ the diagonalizable matrices are precisely the projections, and so we get the same sequence as in section 1.9. From p_1 to p_8 the sequence is

$$2, 8, 58, 802, 20834, 1051586, 102233986, 196144424834.$$

For $q = 3$ the map $P \mapsto P + I$ gives a bijection from the set of projections to the set of diagonalizable matrices with eigenvalues 1 or 2. Such matrices are precisely the solutions of $X^2 = I$. The sequence is given in the OEIS by A053846. From p_1 to p_7 the sequence is

$$1, 2, 14, 236, 12692, 1783784, 811523288, 995733306992.$$

There is a bijection between the set of $n \times n$ projections and the direct sum splittings $\mathbf{F}_q^n = V \oplus W$. The projection P corresponds to the splitting $\mathrm{Im}P \oplus \mathrm{Ker}P$. Note that $V \oplus W$ is regarded as different from $W \oplus V$. Hence,

$$p_n = 2 + 2 \left\{ {n \atop 2} \right\}_q ,$$

because $\left\{ {n \atop 2} \right\}_q$ is the number of splittings into two proper subspaces, with $V \oplus W$ regarded as the same as $W \oplus V$.

From §1.3 we have

$$\binom{n}{k}_q = \frac{\gamma_n}{\gamma_k \gamma_{n-k} q^{k(n-k)}},$$

showing the relationship between the number of subspaces of dimension k and the number of projections of rank k. From it we see that t there are $q^{k(n-k)}$ complementary subspaces for a fixed subspace of dimension k.

1.11 Solutions of $A^k = I$

Let a_n be the number of $n \times n$ matrices A satisfying $A^2 = I$. Such matrices correspond to group homomorphisms from the cyclic group of order 2 to $\mathrm{GL}_n(q)$. In characteristic other than two, the generating function for the a_n is

$$1 + \sum_{n \geq 1} \frac{a_n}{\gamma_n} u^n = \left(\sum_{m \geq 0} \frac{u_m}{\gamma_m} \right)^2 ,$$

and so

$$a_n = \sum_{i=0}^{n} \frac{\gamma_n}{\gamma_i \gamma_{n-i}}.$$

These matrices are those which are diagonalizable and have only 1 and −1 for eigenvalues. If we fix two distinct elements λ_1 and λ_2 in the base field $\mathbf{F}_q$, then a_n also gives the number of diagonalizable matrices having eigenvalues λ_1 and λ_2. Taking the eigenvalues to be 0 and 1 gives the set of projections, and so we see that the number of projections is the same as the number of solutions to $A^2 = I$, when q is not a power of 2. The proof in §2.4 for the number of projections is essentially the proof for the more general case. The sequence A053846 gives the number of solutions over $\mathbf{F}_3$.

In characteristic two, $A^2 = I$ does not imply that A is diagonalizable and the previous formula does not hold. We have the formula

$$a_n = \sum_{0 \le i \le n/2} \frac{\gamma_n}{q^{i(2n-3i)} \gamma_i \gamma_{n-2i}}$$

to be proved in §2.5. Because $A^2 = I$ is equivalent to $(A + I)^2 = 0$, the formula for a_n also counts the number of $n \times n$ nilpotent matrices N such that $N^2 = 0$. For $q = 2$ the sequence is A053722. Although there appears to be an error in the formula given in the OEIS entry, the initial terms of the sequence are correct. For $n = 1, \ldots, 8$ they are

$$1, 4, 22, 316, 6976, 373024, 32252032, 6619979776.$$

For $q = 4$ the sequence is A053856 and the initial terms for $n = 1, \ldots, 7$ are

$$1, 16, 316, 69616, 21999616, 74351051776, 374910580965376.$$

More generally, let k be a positive integer not divisible by p, where q is a power of p. We consider the solutions of $A^k = I$ and let a_n be the number of $n \times n$ solutions with coefficients in $\mathbf{F}_q$. Now $z^k - 1$ factors into a product of distinct irreducible polynomials

$$z^k - 1 = \phi_1(z)\phi_2(z) \cdots \phi_r(z).$$

Let $d_i = \deg \phi_i$. Then the generating function for the a_n is

$$1 + \sum_{n \ge 1} \frac{a_n}{\gamma_n} u^n = \prod_{i=1}^{r} \sum_{m \ge 0} \frac{q^{md_i}}{\gamma_m(q^{d_i})}.$$

Note that a_n counts the homormorphisms from the cyclic group of order k to $\mathrm{GL}_n(q)$. The generating function given here is a special case of the generating function given by Chigira, Takegahara, and Yoshida [3] for the sequence whose nth term is the number of homomorphisms from a finite group G to $\mathrm{GL}_n(q)$ under the assumption that the characteristic of $\mathbf{F}_q$ does not divide the order of G.

Now we consider some specific examples. Let $k = 3$ and let q be a power of 2. Then

$$z^3 - 1 = z^3 + 1 = (z + 1)(z^2 + z + 1)$$

is the irreducible factorization. Thus, $d_1 = 1$ and $d_2 = 2$. The generating function is

$$1 + \sum_{n\geq 1} \frac{a_n}{\gamma_n} u^n = \left(\sum_{m\geq 0} \frac{u^m}{\gamma_m} \right) \left(\sum_{m\geq 0} \frac{u^{2m}}{\gamma_m(q^2)} \right).$$

With $q = 2$ we get the sequence A053725 with initial terms for $n = 1, \ldots, 8$

$$1, 3, 57, 1233, 75393, 19109889, 6326835201, 6388287561729.$$

With $q = 4$ we get the sequence A053857 with initial terms for $n = 1, \ldots, 5$

$$3, 63, 8739, 5790339, 25502129667.$$

For the next example, let $k = 8$ and let q be a power of 3. Then

$$z^8 - 1 = (z-1)(z+1)\phi_3(z)\phi_4(z)\phi_5(z),$$

where the last three factors all have degree 2. Thus, $r = 5$, $d_1 = d_2 = 1$, and $d_3 = d_4 = d_5 = 2$. The generating function is given by

$$\sum_{n\geq 1} \frac{a_n}{\gamma_n} u^n = \left(\sum_{m\geq 0} \frac{u^m}{\gamma_m} \right)^2 \left(\sum_{m\geq 0} \frac{u^{2m}}{\gamma_m(q^2)} \right)^3.$$

For $q = 3$ this gives the sequence A053853 beginning for $n = 1, \ldots, 5$

$$2, 32, 4448, 3816128, 26288771456.$$

These are the sequences in the OEIS for small values of k and q.

k	$q = 2$	$q = 3$	$q = 4$
2	A053722	A053846	A053856
3	A053725	A053847	A053857
4	A053718	A053848	A053859
5	A053770	A053849	A053860
6	A053771	A053851	A053861
7	A053772	A053852	A053862
8	A053773	A053853	A053863
9	A053774	A053854	
10	A053775	A053855	
11	A053776		
12	A053777		

1.12 Nilpotent matrices

Fine and Herstein [5] proved that the number of nilpotent $n \times n$ matrices is $q^{n(n-1)}$, and Gerstenhaber [7] simplified the proof. Recently Crabb has given an even more accessible proof [4]. For $q = 2$ this is sequence A053763 with initial terms from $n = 1$ to $n = 6$

$$1, 1, 4, 64, 4096, 1048576, 1073741824.$$

1.13 Cyclic matrices

A matrix A is **cyclic** if there exists a vector v such that $\{A^i v | i = 0, 1, 2, \ldots\}$ spans the underlying vector space. (The term **regular** is also used.) An equivalent description is that the minimal and characteristic polynomials of A are the same. Let a_n be the number of cyclic matrices over $\mathbf{F}_q$. The generating function factors as

$$1 + \sum_{n \geq 1} \frac{a_n}{\gamma_n} u^n = \prod_{d \geq 1} \left(1 + \frac{1}{q^d - 1} \frac{u^d}{1 - (u/q)^d} \right)^{\nu_d},$$

and can be put into the form

$$1 + \sum_{n \geq 1} \frac{a_n}{\gamma_n} u^n = \frac{1}{1 - u} \prod_{d \geq 1} \left(1 + \frac{u^d}{q^d(q^d - 1)} \right)^{\nu_d},$$

where ν_d is the number of irreducible, monic polynomials of degree d over $\mathbf{F}_q$. The generating function can be extracted from the proof of Theorem 1 in [6], which we present in section 2.

For $q = 2$ the sequence from a_1 to a_7 is

$$2, 14, 412, 50832, 25517184, 51759986688, 422000664182784.$$

Wall [13] proved that the probability that an $n \times n$ matrix is cyclic has a limit

$$\lim_{n \to \infty} \frac{a_n}{q^{n^2}} = \left(1 - \frac{1}{q^5} \right) \prod_{r \geq 3} \left(1 - \frac{1}{q^r} \right).$$

Fulman [6] also has a proof. For $q = 2$ this limit is $0.7403\ldots$.

1.14 Semi-simple matrices

A matrix A is **semi-simple** if it diagonalizes over the algebraic closure of the base field. Let a_n be the number of semi-simple $n \times n$ matrices over $\mathbf{F}_q$. Then the generating function has a factorization

$$1 + \sum_{n \geq 1} \frac{a_n}{\gamma_n} u^n = \prod_{d \geq 1} \left(1 + \sum_{j \geq 1} \frac{u^{jd}}{\gamma_j(q^d)} \right)^{\nu_d},$$

where $\gamma_j(q^d) = |\mathrm{GL}_j(q^d)|$. For $q = 2$ the sequence from a_1 to a_7 is

$$2, 10, 218, 25426, 11979362, 24071588290, 195647202043778.$$

1.15 Separable matrices

A matrix is **separable** if it is both cyclic and semi-simple, which is equivalent to having a characteristic polynomial that is square-free. Let a_n be the number of separable $n \times n$ matrices over $\mathbf{F}_q$. Then the generating function factors

$$1 + \sum_{n \geq 1} \frac{a_n}{\gamma_n} u^n = \prod_{d \geq 1} \left(1 + \frac{u^d}{q^d - 1} \right)^{\nu_d}.$$

This can also be factored as

$$1 + \sum_{n\geq 1} \frac{a_n}{\gamma_n} u^n = \frac{1}{1-u} \prod_{d\geq 1} \left(1 + \frac{u^d(u^d-1)}{q^d(q^d-1)}\right)^{\nu_d}.$$

For $q = 2$ the sequence from a_1 to a_7 is

$$2, 8, 160, 22272, 9744384, 20309999616, 165823024988160.$$

The number of conjugacy classes of separable $n \times n$ matrices is $q^n - q^{n-1}$ for $n \geq 2$ and q for $n = 1$. This is proved by Neumann and Praeger [11, Lemma 3.2] by showing that the number of square-free monic polynomials of degree n is $q^n - q^{n-1}$. There is a natural bijection between the set of conjugacy classes of separable matrices and the set of square-free monic polynomials obtained by associating to each conjugacy class the characteristic polynomial of the matrices in that class.

1.16 Conjugacy classes

Let a_n be the number of conjugacy classes of $n \times n$ matrices over $\mathbf{F}_q$. The generating function for this sequence is

$$1 + \sum_{n\geq 1} a_n u^n = \prod_{r\geq 1} \frac{1}{1-qu^r}.$$

The number of conjugacy classes grows like q^n. In fact,

$$\lim_{n\to\infty} \frac{a_n}{q^n} = \prod_{r\geq 1} \left(1 - \frac{1}{q^r}\right)^{-1},$$

which is the reciprocal of the limiting probability that a matrix is invertible. See section 1.2.

For $q = 2$ the sequence is A070933. The initial terms for $n = 1, \ldots, 10$ are

$$2, 6, 14, 34, 74, 166, 350, 746, 1546, 3206.$$

For $q = 3$ the initial terms for $n = 1, \ldots, 10$ are

$$3, 12, 39, 129, 399, 1245, 3783, 11514, 34734, 104754.$$

Let b_n be the number of conjugacy classes in the general linear group $\mathrm{GL}_n(q)$, the group of $n \times n$ invertible matrices over $\mathbf{F}_q$. Then

$$1 + \sum_{n\geq 0} b_n u^n = \prod_{r\geq 1} \frac{1-u^r}{1-qu^r}.$$

For $q = 2$ the sequence is A006951, which starts

$$1, 3, 6, 14, 27, 60, 117, 246, 490, 1002.$$

For $q = 3$ the sequence is A006952, which starts

$$2, 8, 24, 78, 232, 720, 2152, 6528, 19578, 58944.$$

For $q = 4, 5, 7$ the sequences are A049314, A049315, and A049316.

The number of conjugacy classes is asymptotic to q^n:

$$\lim_{n\to\infty} \frac{b_n}{q^n} = 1.$$

Hence, in the limit the ratio of the number of conjugacy classes of invertible matrices to the number of conjugacy classes of all matrices is the same as the limiting probability that a matrix is invertible. That is,

$$\lim_{n\to\infty} \frac{b_n}{a_n} = \prod_{r\geq 1} \left(1 - \frac{1}{q^r}\right).$$

Sequence A070731 gives the size of the largest conjugacy class in $\mathrm{GL}_n(2)$. Starting with $n = 1$ the initial terms are

$$1, 3, 56, 3360, 833280, 959938560.$$

The minimal order of the centralizers of elements in $\mathrm{GL}_n(2)$ is given by the quotient of γ_n by the nth term in this sequence. The resulting sequence for $n = 1, \dots 10$ is

$$1, 2, 3, 6, 12, 21, 42, 84, 147, 294.$$

This sequence is A082877 in the OEIS.

2 Selected Proofs

2.1 The cycle index and generating functions

In sections 1.6-1.13 we make heavy use of generating functions of the form

$$1 + \sum_{n\geq 1} \frac{a_n}{\gamma_n} u^n,$$

where the sequence a_n counts some class of $n \times n$ matrices. These generating functions come from the **cycle index** for matrices that was first defined by Kung [9] and later extended by Stong [12]. We follow Fulman's notation in [6]. The cycle index for conjugation action of $\mathrm{GL}_n(q)$ on $\mathrm{M}_n(q)$ is a polynomial in the indeterminates $x_{\phi,\lambda}$, where ϕ ranges over the set Φ of monic irreducible polynomials over $\mathbf{F}_q$ and λ ranges over the partitions of the positive integers. First we recall that the conjugacy class of a matrix A is determined by the isomorphism type of the associated $\mathbf{F}_q[z]$-module on the vector space $\mathbf{F}_q^n$ in which the action of z is that of A. This module is isomorphic to a direct sum

$$\bigoplus_{i=1}^{k} \bigoplus_{j=1}^{l_i} \mathbf{F}_q[z]/(\phi_i^{\lambda_{i,j}})$$

where $\phi_1, \ldots, \phi_k$ are distinct monic irreducible polynomials; for each i, $\lambda_{i,1} \geq \lambda_{i,2} \geq \cdots \geq \lambda_{i,l_i}$ is a partition of $n_i = \sum_j \lambda_{i,j}$. Since A is $n \times n$, then $n = \sum_i n_i \deg \phi_i = \sum_{i,j} \lambda_{i,j} \deg \phi_i$. Let λ_i denote the partition of n_i given by the $\lambda_{i,j}$ and define $|\lambda_i| = n_i$. The conjugacy class of A in $\mathrm{M}_n(q)$ is determined by the data consisting of the finite list of distinct monic irreducible polynomials $\phi_1, \ldots, \phi_k$ and the partitions $\lambda_1, \ldots, \lambda_k$.

The cycle index is defined to be

$$\frac{1}{\gamma_n} \sum_{A \in \mathrm{M}_n(q)} \prod_{\phi \in \Phi} x_{\phi, \lambda_\phi(A)},$$

where $\lambda_\phi(A)$ is the partition associated to ϕ in the conjugacy class data for A. If ϕ does not occur in the polynomials associated to A, then $\lambda_\phi(A)$ is the empty partition, and we define $x_{\phi,\lambda_\phi(A)} = 1$.

We construct the generating function for the cycle index

$$1 + \sum_{n \geq 1} \frac{u^n}{\gamma_n} \sum_{A \in \mathrm{M}_n(q)} \prod_{\phi \in \Phi} x_{\phi, \lambda_\phi(A)}.$$

This generating function has a formal factorization over the monic irreducible polynomials. For the proof we refer to the paper of Stong [12, p. 170] .

Lemma 1

$$1 + \sum_{n=1}^{\infty} \frac{u^n}{\gamma_n} \sum_{A \in \mathrm{M}_n(q)} \prod_{\phi} x_{\phi, \lambda_\phi(A)} = \prod_{\phi} \sum_{\lambda} \frac{x_{\phi,\lambda} u^{|\lambda| \deg \phi}}{c_\phi(\lambda)}$$

where $c_\phi(\lambda)$ is the order of the group of module automorphisms of the $\mathbf{F}_q[z]$-module $\bigoplus_j \mathbf{F}_q[z]/(\phi^{\lambda_j})$.

Lemma 2 *Fix a monic irreducible ϕ. Then*

$$\sum_{\lambda} \frac{u^{|\lambda| \deg \phi}}{c_\phi(\lambda)} = \prod_{r \geq 1} \left(1 - \frac{u^{\deg \phi}}{q^{r \deg \phi}}\right)^{-1}.$$

Proof We use the formula for $c_\phi(\lambda)$ proved by Kung [9, Lemma 2, p. 146]. Let λ be a partition of n and let b_i be the number of parts of size i. Let $d_i = b_1 + 2b_2 + \cdots + ib_i + i(b_{i+1} + \cdots + b_n)$. Then

$$c_\phi(\lambda) = \prod_i \prod_{k=1}^{b_i} (q^{d_i \deg \phi} - q^{(d_i - k) \deg \phi}).$$

We see from this formula that $c_\phi(\lambda)$ is a function of λ and $q^{\deg \phi}$. Therefore it is sufficient to prove the lemma for a single polynomial of degree 1, say $\phi(z) = z$, and then to replace u by $u^{\deg \phi}$ and q by $q^{\deg \phi}$. So, now we will prove that for $\phi(z) = z$,

$$\sum_{\lambda} \frac{u^{|\lambda|}}{c_\phi(\lambda)} = \prod_{r \geq 1} \left(1 - \frac{u}{q^r}\right)^{-1}.$$

We split the left side into an outer sum over n and an inner sum over the partitions of n

$$\sum_{\lambda} \frac{u^{|\lambda|}}{c_\phi(\lambda)} = 1 + \sum_{n\geq 1} \sum_{|\lambda|=n} \frac{u^n}{c_\phi(\lambda)}.$$

To evaluate the inner sum we note that $\gamma_n \sum_{|\lambda|=n} \frac{1}{c_\phi(\lambda)}$ is the number of $n \times n$ nilpotent matrices, which is $q^{n(n-1)}$ from the theorem of Fine and Herstein [5]. Therefore, the u^n coefficient of the left side is

$$\sum_{|\lambda|=n} \frac{1}{c_\phi(\lambda)} = \frac{1}{q^n(1-\frac{1}{q})\ldots(1-\frac{1}{q^n})}.$$

For the right side we use a formula of Euler, which is a special case of Cauchy's identity and a limiting case of the q-binomial theorem. A convenient reference is the book of Hardy and Wright [8, Theorem 349, p. 280]. For $|a| < 1$, $|y| < 1$, the coefficient of a^n in the infinite product

$$\prod_{r\geq 1} \frac{1}{(1-ay^r)}$$

is

$$\frac{y^n}{(1-y)(1-y^2)\ldots(1-y^n)}.$$

Let $a = u$ and $y = \frac{1}{q}$ to see that the u^n coefficient of

$$\prod_{r\geq 1} \left(1 - \frac{u}{q^r}\right)^{-1}$$

is

$$\frac{1}{q^n(1-\frac{1}{q})\ldots(1-\frac{1}{q^n})}.$$

Therefore, the coefficients of u^n of the left and right sides are equal and so we have proved that for $\phi(z) = z$,

$$\sum_{\lambda} \frac{u^{|\lambda|}}{c_\phi(\lambda)} = \prod_{r\geq 1} \left(1 - \frac{u}{q^r}\right)^{-1}.$$

□

Lemma 3 *Let Φ' be a subset of the irreducible monic polynomials. Let a_n be the number of $n \times n$ matrices whose conjugacy class data involves only polynomials $\phi \in \Phi'$. Then*

$$1 + \sum_{n\geq 1} \frac{a_n}{\gamma_n} u^n = \prod_{\phi\in\Phi'} \sum_{\lambda} \frac{u^{|\lambda| \deg \phi}}{c_\phi(\lambda)}$$

$$1 + \sum_{n\geq 1} \frac{a_n}{\gamma_n} u^n = \prod_{\phi\in\Phi'} \prod_{r\geq 1} \left(1 - \frac{u^{\deg \phi}}{q^{r \deg \phi}}\right)^{-1}.$$

Proof Using Lemma 1 we set $x_{\phi,\lambda} = 1$ or 0 according to whether $\phi \in \Phi'$ or not. Then on the left side the inner sum is over the matrices A that do not have factors of $\phi \in \Phi'$ in their characteristic polynomials, and so the coefficient of u^n is simply the number of such $n \times n$ matrices. This gives the first equality in the statement of the lemma

$$1 + \sum_{n \geq 1} \frac{a_n}{\gamma_n} u^n = \prod_{\phi \in \Phi'} \sum_{\lambda} \frac{u^{|\lambda| \deg \phi}}{c_\phi(\lambda)}.$$

Then from Lemma 2 we get the second equality. □

Lemma 4

$$\frac{1}{1-u} = \prod_{\phi \neq z} \sum_{\lambda} \frac{u^{|\lambda| \deg \phi}}{c_\phi(\lambda)}$$

$$\frac{1}{1-u} = \prod_{\phi \neq z} \prod_{r \geq 1} \left(1 - \frac{u^{\deg \phi}}{q^{r \deg \phi}}\right)^{-1}.$$

Proof Using Lemma 3 we let Φ' be the complement of the polynomial $\phi(z) = z$. The matrices not having factors of z in their characteristic polynomials are the invertible matraices. Thus, $a_n = \gamma_n$, and so the left side is $1 + \sum_{n \geq 1} u^n$. □

We can generalize the first part of Lemma 3 to allow for conjugacy class data in which the allowed partitions vary with the polynomials. The proof follows immediately from Lemma 1.

Lemma 5 *For each monic, irreducible polynomial ϕ let L_ϕ be a subset of all partitions of the positive integers. Let a_n be the number of $n \times n$ matrices A such that $\lambda_\phi(A) \in L_\phi$ for all ϕ. Then*

$$1 + \sum_{n \geq 1} \frac{a_n}{\gamma_n} u^n = \prod_{\phi} \sum_{\lambda \in L_\phi} \frac{u^{|\lambda| \deg \phi}}{c_\phi(\lambda)}.$$

Lemma 6

$$1 - u = \prod_{\phi} \left(1 - \frac{u^{\deg \phi}}{q^{\deg \phi}}\right) = \prod_{d \geq 1} \left(1 - \frac{u^d}{q^d}\right)^{\nu_d}$$

Proof Unique factorization in the ring of polynomials $\mathbf{F}_q[z]$ means that each of the q^n monic polynomials of degree n has a unique factorization as a product of monic irreducible polynomials. This implies the factorization of the generating function

$$\sum_{n \geq 0} q^n u^n = \prod_{\phi} \sum_{k \geq 0} u^{k \deg \phi}.$$

The left side and the inner sum on the right are geometric series, and so

$$\frac{1}{1 - qu} = \prod_{\phi} \frac{1}{1 - u^{\deg \phi}}.$$

Grouping the factors on the right according to degree we get

$$\frac{1}{1-qu} = \prod_{d\geq 1} \left(\frac{1}{1-u^d}\right)^{\nu_d}.$$

Substituing u/q for u gives

$$\frac{1}{1-u} = \prod_{d\geq 1} \left(\frac{1}{1-(u/q)^d}\right)^{\nu_d}.$$

The lemma follows by taking reciprocals. □

The final lemma below is used to evaluate limiting probabilities such as $\lim_{n\to\infty} a_n/\gamma_n$. The proof is straightforward and omitted.

Lemma 7 *If*

$$\sum_{n\geq 0} \alpha_n u^n = \frac{1}{1-u} F(u)$$

where $F(u)$ is analytic and the series for $F(1)$ is convergent, then

$$\lim_{n\to\infty} \alpha_n = F(1).$$

Now with these lemmas we are ready to prove several results stated in §1.

2.2 Linear and Projective Derangements

In this section we prove the results given in §1.8. Linear derangements are matrices with no eigenvalues of 0 or 1, which means that their characteristic polynomials do not have factors of z or $z-1$.

Theorem 8 *Let e_n be the number of $n \times n$ linear derangements. Then*

$$1 + \sum_{n\geq 1} \frac{e_n}{\gamma_n} u^n = \frac{1}{1-u} \prod_{r\geq 1} \left(1 - \frac{u}{q^r}\right).$$

Proof In Lemma 3 let $\Phi' = \Phi \setminus \{z, z-1\}$ to see that

$$1 + \sum_{n\geq 1} \frac{e_n}{\gamma_n} u^n = \prod_{\phi\in\Phi'} \prod_{r\geq 1} \left(1 - \frac{u^{\deg\phi}}{q^{r\deg\phi}}\right)^{-1}.$$

On the right side multiply and divide by the product corresponding to $\phi(z) = z$, which is

$$\prod_{r\geq 1} \left(1 - \frac{u}{q^r}\right)^{-1},$$

to see that

$$1 + \sum_{n\geq 1} \frac{e_n}{\gamma_n} u^n = \prod_{\phi\neq z} \prod_{r\geq 1} \left(1 - \frac{u^{\deg\phi}}{q^{r\deg\phi}}\right)^{-1} \prod_{r\geq 1} \left(1 - \frac{u}{q^r}\right).$$

Then use Lemma 4 to give

$$1+\sum_{n\geq 1}\frac{e_n}{\gamma_n}u^n=\frac{1}{1-u}\prod_{r\geq 1}\left(1-\frac{u}{q^r}\right).$$

□

From the generating function we can derive a recursive formula for e_n.

Corollary 9

$$e_n=e_{n-1}(q^n-1)q^{n-1}+(-1)^n q^{n(n-1)/2},\ e_0=1.$$

Proof From Theorem 8 it follows that e_n/γ_n is the sum of the u^i coefficients of

$$\prod_{r\geq 1}(1-u/q^r)$$

for $i=0,1,\ldots,n$. Now the u^i coefficient is

$$(-1)^i\sum_{1\leq r_1<r_2<\cdots<r_i}\frac{1}{q^{r_1+r_2+\cdots+r_i}}.$$

By induction one can easily show that this coefficient is

$$\frac{(-1)^i}{(q^i-1)(q^{i-1}-1)\cdots(q-1)}.$$

Therefore

$$\frac{e_n}{\gamma_n}=1+\sum_{1\leq i\leq n}\frac{(-1)^i}{(q^i-1)(q^{i-1}-1)\cdots(q-1)}.$$

Next,

$$\frac{e_n}{\gamma_n}=\frac{e_{n-1}}{\gamma_{n-1}}+\frac{(-1)^n}{(q^n-1)\cdots(q-1)}.$$

Making use of the formula for γ_n and γ_{n-1} and canceling where possible we see that

$$e_n=e_{n-1}(q^n-1)q^{n-1}+(-1)^n q^{n(n-1)/2}.$$

□

We present the next result because the sequence e_n for $q=2$ is given in the OEIS as $2^{n(n-1)/2}a_n$ where a_n satisfies a recursive formula.

Corollary 10 *Let*

$$a_n=\frac{e_n}{q^{n(n-1)/2}}.$$

Then a_n satisfies the recursion

$$a_n=a_{n-1}(q^n-1)+(-1)^n,\ a_0=1.$$

Proof The proof follows immediately from the recursive formula for e_n. □

Corollary 11 *The asymptotic probability that an invertible matrix is a linear derangement is*

$$\lim_{n\to\infty} \frac{e_n}{\gamma_n} = \prod_{r\geq 1}\left(1-\frac{1}{q^r}\right).$$

The asymptotic that any matrix is a linear derangement is

$$\lim_{n\to\infty} \frac{e_n}{q^{n^2}} = \prod_{r\geq 1}\left(1-\frac{1}{q^r}\right)^2.$$

Proof We use Lemma 7 for the first statement. Then

$$\begin{aligned}\lim_{n\to\infty} \frac{e_n}{q^{n^2}} &= \lim_{n\to\infty} \frac{e_n}{\gamma_n}\frac{\gamma_n}{q^{n^2}} \\ &= \left(\lim_{n\to\infty} \frac{e_n}{\gamma_n}\right)\left(\lim_{n\to\infty} \frac{\gamma_n}{q^{n^2}}\right).\end{aligned}$$

We have just computed the first limit on the right and the second limit (from §1.2) is the same. □

The proof of Theorem 8 easily adapts to give the generating function for the number of projective derangements.

Theorem 12 *Let d_n be the number of $n \times n$ projective derangements. Then*

$$1+\sum_{n\geq 1}\frac{d_n}{\gamma_n}u^n = \frac{1}{1-u}\prod_{r\geq 1}\left(1-\frac{u}{q^r}\right)^{q-1}.$$

Proof In this case $\Phi' = \Phi \setminus \{z-a | a \in \mathbf{F}_q\}$. As in the proof of Theorem 8 this time we multiply and divide by the products corresponding to all the linear polynomials except $\phi(z) = z-1$. There are $q-1$ of these and so we get

$$1+\sum_{n\geq 1}\frac{e_n}{\gamma_n}u^n = \prod_{\phi\neq z}\prod_{r\geq 1}\left(1-\frac{u^{\deg\phi}}{q^{r\deg\phi}}\right)^{-1}\prod_{r\geq 1}\left(1-\frac{u}{q^r}\right)^{q-1}.$$

Use Lemma 4 to finish the proof. □

It would be interesting to find a recursive formula for the d_n analagous to that given in Corollary 9 for the e_n.

2.3 Diagonalizable matrices

Theorem 13 *Let d_n be the number of diagonalizable $n \times n$ matrices. Then*

$$1+\sum_{n\geq 0}\frac{d_n}{\gamma_n}u^n = \left(\sum_{m\geq 0}\frac{u^m}{\gamma_m}\right)^q$$

and

$$d_n = \sum_{n_1+\cdots+n_q=n}\frac{\gamma_n}{\gamma_{n_1}\cdots\gamma_{n_q}}.$$

Proof We use Lemma 5. Diagonalizable matrices have conjugacy class data that only involves the linear polynomials $\phi(z) = z - a$, $a \in \mathbf{F}_q$ and partitions $\lambda_\phi(A)$ that are either empty or have the form $1 \geq 1 \geq \ldots \geq 1$. These partitions are indexed by non-negative integer. For $\phi(z) = z - a$ and for λ the partition consisting of m 1's, the corresponding $m \times m$ matrix in the canonical form is the diagonal matrix with a on the main diagonal. The centralizer subgroup of this matrix is the full general linear group $\mathrm{GL}_m(q)$ and so $c_\phi(\lambda) = \gamma_m$. Then from Lemma 5 we see that

$$\begin{aligned} 1 + \sum_{n \geq 0} \frac{d_n}{\gamma_n} u^n &= \prod_{a \in \mathbf{F}_q} \sum_{m \geq 0} \frac{u^m}{\gamma_m} \\ &= \left(\sum_{m \geq 0} \frac{u^m}{\gamma_m} \right)^q . \end{aligned}$$

From this the formula for d_n follows immediately. □

It should be noted that the formula for d_n follows directly from the knowledge of the centralizer subgroup of a diagonalizable matrix and does not require the full machinery of the cycle index generating function. Also, there is an alternative approach to this problem given in [10].

2.4 Projections

Theorem 14 *Let p_n be the number of $n \times n$ projections. Then*

$$1 + \sum_{n \geq 0} \frac{p_n}{\gamma_n} u^n = \left(\sum_{m \geq 0} \frac{u^m}{\gamma_m} \right)^2$$

and

$$p_n = \sum_{0 \leq i \leq n} \frac{\gamma_n}{\gamma_i \gamma_{n-i}}.$$

Proof Since projections are diagonalizable matrices with eigenvalues restricted to be in the set $\{0, 1\}$, it follows that the product in the generating function for the cycle index is over the two polynomials z and $z - 1$ and the partitions are restricted as described in the previous theorem. Thus, we see that

$$\begin{aligned} 1 + \sum_{n \geq 0} \frac{p_n}{\gamma_n} u^n &= \prod_{z, z-1} \sum_{m \geq 0} \frac{u^m}{\gamma_m} \\ &= \left(\sum_{m \geq 0} \frac{u^m}{\gamma_m} \right)^2 . \end{aligned}$$

The formula for p_n follows immediately. □

2.5 Solutions of $A^k = I$

Theorem 15 *Let a_n be the number of $n \times n$ matrices A satisfying $A^2 = I$, and assume that the base field $\mathbf{F}_q$ has characteristic two. Then*

$$a_n = \sum_{0 \le i \le n/2} \frac{\gamma_n}{q^{i(2n-3i)}\gamma_i \gamma_{n-2i}}.$$

Proof The rational canonical form for A is a direct sum of companion matrices for $z-1$ and $(z-1)^2$. No other polynomials occur. Thus, the partition $\lambda_\phi(A)$ for $\phi(z) = z-1$ consists of b_1 repetitions of 1 and b_2 repetitions of 2, where $b_1 + 2b_2 = n$. From Lemma 5 we see that

$$1 + \sum_{n \ge 1} \frac{a_n}{\gamma_n} u^n = \sum_{b_1,\, b_2} \frac{u^{b_1+2b_2}}{c_{z-1}(b)},$$

where $b = (b_1, b_2)$ denotes the partition. To compute $c_{z-1}(b)$ we refer to the formula stated in the proof of Lemma 2. In that formula we have $d_1 = b_1 + b_2$ and $d_2 = b_1 + 2b_2$, and then

$$c_{z-1}(b) = \prod_{i=1}^{2} \prod_{k=1}^{b_i} (q^{d_i} - q^{d_i-k}).$$

This becomes

$$c_{z-1}(b) = \prod_{k=1}^{b_1} (q^{d_1} - q^{d_1-k}) \prod_{k=1}^{b_2} (q^{d_2} - q^{d_2-k}).$$

Now let $i = d_1 - k$ in the first product and let $i = d_2 - k$ in the second product, so that

$$c_{z-1}(b) = \prod_{i=b_2}^{d_1-1} (q^{d_1} - q^i) \prod_{i=d_2-b_2}^{d_2-1} (q^{d_2} - q^i).$$

From each factor of the first product we pull out a factor of q^{b_2} and from each factor of the second product we remove a factor of $q^{d_2-b_2}$. This gives

$$c_{z-1}(b) = q^{b_1 b_2} \gamma_{b_1} q^{(d_2-b_2)b_2} \gamma_{b_2}.$$

Then

$$\frac{a_n}{\gamma_n} = \sum_{b_1+2b_2=n} \frac{1}{c_{z-1}(b)},$$

where we note that $d_2 = n$ and $b_1 = n - 2b_2$. Therefore,

$$\frac{a_n}{\gamma_n} = \sum_{b_1+2b_2=n} \frac{1}{q^{b_2(3n-2b_2)}\gamma_{b_1}\gamma_{b_2}},$$

which is equivalent to the formula to be proved. □

Theorem 16 *Assume that k is a positive integer relatively prime to q. Let*

$$z^k - 1 = \phi_1(z)\phi_2(z)\cdots\phi_r(z)$$

be the factorization of z^k-1 over $\mathbf{F}_q$ into distinct irreducible polynomials with $d_i = \deg\phi_i$, and let a_n be the number of $n\times n$ matrices over $\mathbf{F}_q$ that are solutions of $A^k = I$. Then

$$1 + \sum_{n\geq 1} \frac{a_n}{\gamma_n} u^n = \prod_{i=1}^{r} \sum_{m\geq 0} \frac{q^{md_i}}{\gamma_m(q^{d_i})}.$$

Proof The rational canonical form of a matrix A satisfying $A^k = I$ is a direct sum of any number of copies of the companion matrices of the ϕ_i. Thus, with Lemma 5 the product is taken over the ϕ_i for $i = 1,\ldots,r$ and the subset L_{ϕ_i} is the same for all i and consists of the partitions in which all parts are 1. Hence, L_{ϕ_i} can be identified with the non-negative integers $m = 0,1,2,\ldots$. For the partition λ given by m 1's, the value of $c_{\phi_i}(\lambda)$ is the order of the group of automorphisms of the $\mathbf{F}_q[z]$-module $\mathbf{F}_q[z]/(\phi_i^m)$, but this module is the direct sum of m copies of the extension field of degree d_i over $\mathbf{F}_q$. Therefore, the group of automorphisms is the general linear group $\mathrm{GL}_m(q^{d_i})$, and so $c_{\phi_i}(\lambda) = \gamma_m(q^{d_i})$. □

2.6 Cyclic matrices

Theorem 17 *Let a_n be the number of cyclic $n\times n$ matrices. Then*

$$1 + \sum_{n\geq 1} \frac{a_n}{\gamma_n} u^n = \prod_{d\geq 1} \left(1 + \frac{1}{q^d-1}\,\frac{u^d}{1-(u/q)^d}\right)^{\nu_d}$$

and

$$1 + \sum_{n\geq 1} \frac{a_n}{\gamma_n} u^n = \frac{1}{1-u} \prod_{d\geq 1} \left(1 + \frac{u^d}{q^d(q^d-1)}\right)^{\nu_d}.$$

Proof In terms of the conjugacy class data a matrix is cyclic if λ_ϕ has at most one part for each ϕ. Thus, $L_\phi = \{\emptyset, 1, 2, \ldots\}$, where m means the partition of m having just one part. For these partitions we have $c_\phi(\emptyset) = 1$ and $c_\phi(m) = q^{m\deg\phi} - q^{(m-1)\deg\phi}$. Let a_n be the number of cyclic matrices of size $n\times n$. Beginning with Lemma 5 we find the generating function.

$$\begin{aligned}
1+\sum_{n\geq 1}\frac{a_n}{\gamma_n}u^n &= \prod_{\phi}\sum_{L_\phi}\frac{u^{|\lambda|\deg\phi}}{c_\phi(\lambda)}\\
&= \prod_{\phi}\left(1+\sum_{m\geq 1}\frac{u^{m\deg\phi}}{q^{m\deg\phi}-q^{(m-1)\deg\phi}}\right)\\
&= \prod_{d\geq 1}\left(1+\sum_{m\geq 1}\frac{u^{md}}{q^{md}-q^{(m-1)d}}\right)^{\nu_d}\\
&= \prod_{d\geq 1}\left(1+\frac{1}{q^d-1}\sum_{m\geq 1}\frac{u^{md}}{q^{(m-1)d}}\right)^{\nu_d}\\
&= \prod_{d\geq 1}\left(1+\frac{1}{q^d-1}\frac{u^d}{1-(u/q)^d}\right)^{\nu_d}.
\end{aligned}$$

For the second part, we use Lemma 6 to get

$$1+\sum_{n\geq 1}\frac{a_n}{\gamma_n}u^n = \frac{1}{1-u}\prod_{d\geq 1}\left(1-\frac{u^d}{q^d}\right)^{\nu_d}\prod_{d\geq 1}\left(1+\frac{1}{q^d-1}\frac{u^d}{1-(u/q)^d}\right)^{\nu_d}.$$

Combine the products and simplify to finish the proof. □

2.7 Semi-simple matrices

Theorem 18 *Let a_n be the number of $n\times n$ semi-simple matrices over $\mathbf{F}_q$. Then*

$$1+\sum_{n\geq 1}\frac{a_n}{\gamma_n}u^n = \prod_{d\geq 1}\left(1+\sum_{j\geq 1}\frac{u^{jd}}{\gamma_j(q^d)}\right)^{\nu_d}.$$

Proof In order for a matrix to be semi-simple the partition associated to a polynomial ϕ has no parts greater than 1. Thus, for all ϕ, $L_\phi=\{\emptyset,1,1^2,\ldots,1^j,\ldots\}$, where 1^j means the partition of j consisting of j copies of 1. Then $c_\phi(1^j)$ is the order of the automorphism group of the $\mathbf{F}_q[z]$-module which is the direct sum of j copies of $\mathbf{F}_q[z]/(\phi)$, which can be identified with $(\mathbf{F}_{q^d})^j$, where $d=\deg\phi$. Furthermore, the automorphisms of the module $(\mathbf{F}_q[z]/(\phi))^{\oplus j}$ can be identified with the $\mathbf{F}_{q^d}$-linear automorphisms of $(\mathbf{F}_{q^d})^j$. This group of automorphisms is $\mathrm{GL}_j(q^d)$, and so $c_\phi(1^j)=\gamma_j(q^d)$.

From Lemma 5 we find

$$\begin{aligned}
1+\sum_{n\geq 1}\frac{a_n}{\gamma_n}u^n &= \prod_{\phi}\sum_{L_\phi}\frac{u^{|\lambda|\deg\phi}}{c_\phi(\lambda)}\\
&= \prod_{\phi}\left(1+\sum_{j\geq 1}\frac{u^{j\deg\phi}}{\gamma_j(q^d)}\right)\\
&= \prod_{d\geq 1}\left(1+\sum_{j\geq 1}\frac{u^{jd}}{\gamma_j(q^d)}\right)^{\nu_d}.
\end{aligned}$$

□

2.8 Separable matrices

Theorem 19 *Let a_n be the number of separable $n \times n$ matrices over $\mathbf{F}_q$. Then*

$$1 + \sum_{n \geq 1} \frac{a_n}{\gamma_n} u^n = \prod_{d \geq 1} \left(1 + \frac{u^d}{q^d - 1}\right)^{\nu_d}$$

and

$$1 + \sum_{n \geq 1} \frac{a_n}{\gamma_n} u^n = \frac{1}{1-u} \prod_{d \geq 1} \left(1 + \frac{u^d(u^d-1)}{q^d(q^d - 1)}\right)^{\nu_d}.$$

Proof For a matrix to be separable the allowed partitions are either empty or the unique partition of 1. So the sum over L_ϕ in Lemma 5 is a sum of two terms. For $\lambda = \emptyset$,

$$\frac{u^{|\lambda| \deg \phi}}{c_\phi(\lambda)} = 1,$$

and for $\lambda = 1$,

$$\frac{u^{|\lambda| \deg \phi}}{c_\phi(\lambda)} = \frac{u^{\deg \phi}}{q^{\deg \phi} - 1}.$$

Therefore,

$$\begin{aligned} 1 + \sum_{n \geq 1} \frac{a_n}{\gamma_n} u^n &= \prod_{\phi} \sum_{L_\phi} \frac{u^{|\lambda| \deg \phi}}{c_\phi(\lambda)} \\ &= \prod_{\phi} \left(1 + \frac{u^{\deg \phi}}{q^{\deg \phi} - 1}\right) \\ &= \prod_{d \geq 1} \left(1 + \frac{u^d}{q^d - 1}\right)^{\nu_d}. \end{aligned}$$

For the second statement of the theorem multiply the right side in the line above by

$$\frac{1}{1-u} \prod_{d \geq 1} \left(1 - \frac{u^d}{q^d}\right)^{\nu_d},$$

which is equal to 1 by Lemma 6. Then combine the products. □

2.9 Conjugacy classes

Theorem 20 *Let a_n be the number of conjugacy classes of $n \times n$ matrices. Then the ordinary generating function for the sequence $\{a_n\}$ is given by*

$$1 + \sum_{n \geq 1} a_n u^n = \prod_{r \geq 1} \frac{1}{1 - qu^r}.$$

Proof Recall the ordinary power series generating function for partitions factors as the infinite product

$$\sum_{n\geq 0} p_n u^n = \prod_{r\geq 1} \frac{1}{1-u^r},$$

where p_n is the number of partitions of the integer n. A conjugacy class of $n \times n$ matrices is uniquely specified by the choice of a partition λ_ϕ for each monic irreducible polynomial ϕ such that $\sum_\phi |\lambda_\phi| \deg \phi = n$. Consider the infinite product over ϕ

$$\prod_{\phi} \sum_{n\geq 0} p_n u^{n \deg \phi}.$$

The coefficient of u^n is a sum of terms of the form $p_{n_1} u^{n_1 \deg \phi_1} \cdots p_{n_k} u^{n_k \deg \phi_k}$ where $n = \sum n_k \deg \phi_k$. Therefore, the u^n-coefficient is the number of conjugacy classes of $n \times n$ matrices. Then

$$\begin{aligned} 1 + \sum_{n\geq 1} a_n u^n &= \prod_{\phi} \sum_{n\geq 0} p_n u^{n \deg \phi} \\ &= \prod_{\phi} \prod_{r\geq 1} \frac{1}{1-u^{r \deg \phi}} \\ &= \prod_{r\geq 1} \prod_{\phi} \frac{1}{1-u^{r \deg \phi}} \\ &= \prod_{r\geq 1} \prod_{d\geq 1} \left(\frac{1}{1-u^{rd}}\right)^{\nu_d} \end{aligned}$$

Then by substituting qu^r for u in Lemma 6 and inverting we see that

$$\prod_{d\geq 1} \left(\frac{1}{1-u^{rd}}\right)^{\nu_d} = \frac{1}{1-qu^r}.$$

Therefore

$$1 + \sum_{n\geq 1} a_n u^n = \prod_{r\geq 1} \frac{1}{1-qu^r}.$$

□

References

[1] Edward A. Bender and Jay R. Goldman, Enumerative uses of generating functions, *Indiana Univ. Math. J.* **20** (1970/1971), 753–765.

[2] Peter J. Cameron, *Combinatorics: Topics, Techniques, Algorithms*, Cambridge University Press, Cambridge, 1994.

[3] Naoki Chigira, Yugen Takegahara, and Tomoyuki Yoshida, On the number of homomorphisms from a finite group to a general linear group, *J. Algebra* **232** (2000), 236–254.

[4] M. C. Crabb, Counting nilpotent endomorphisms, *Finite Fields Appl.* **12** (2006), 151–154.

[5] N. J. Fine and I. N. Herstein, The probability that a matrix be nilpotent, *Illinois J. Math.* **2** (1958), 499–504.

[6] Jason Fulman, Random matrix theory over finite fields, *Bull. Amer. Math. Soc. (N.S.)* **39** (2002), 51–85 (electronic).

[7] Murray Gerstenhaber, On the number of nilpotent matrices with coefficients in a finite field, *Illinois J. Math.* **5** (1961), 330–333.

[8] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, fifth ed., The Clarendon Press Oxford University Press, New York, 1979.

[9] Joseph P. S. Kung, The cycle structure of a linear transformation over a finite field, *Linear Algebra Appl.* **36** (1981), 141–155.

[10] Kent E. Morrison, q-exponential families, *Electron. J. Combin.* **11** (2004), Research Paper 36, 11 pp. (electronic).

[11] Peter M. Neumann and Cheryl E. Praeger, Cyclic matrices over finite fields, *J. London Math. Soc.* **52** (1995), 263–284.

[12] Richard Stong, Some asymptotic results on finite vector spaces, *Adv. in Appl. Math.* **9** (1988), 167–199.

[13] G. E. Wall, Counting cyclic and separable matrices over a finite field, *Bull. Austral. Math. Soc.* **60** (1999), 253–284.

Sequences considered: A002416, A002820, A002884, A005329, A006116 –A006122, A015195–A015217, A022166–A022188, A053718, A053722, A053725, A053770–A053777, A053763, A053846–A053849, A053851–A053857, A053859–A053863, A069777, A070933, A076831, A082877.