Enumeration of Matrices over Finite Fields

Geoffrey Critzer

Abstract

We follow [2] in using the idea of the **cycle index** for matrices developed in [1] to derive bivariate generating functions that give enumeration results on matrices over a finite field having various properties. In like manner, we count the number of elements of any given order in $GL_n(\mathbb{F}_q)$. We provide references to some sequences, newly added to the Online Enclyclopedia of Integer Sequences, OEIS. Our presentation provides a concise and uniform mechanism for solving matrix enumeration problems where the desired matrices have properties shared by entire similarity classes.

Introduction

The cycle index for matrices is a "vector space analog of the Polya cycle index for a permutation group"[1]. A beautiful exposition of which is given by Morrison [section 2.1]. In its barest form the cycle index for matrices can be expressed as

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

where the indeterminates are subscripted by an irreducible polynomial ϕ paired with an integer partition $\lambda_\phi(A)$ associated with an $n\times n$ matrix A over a finite field $\mathbb{F}_q$ and $\gamma_n = |GL_n(\mathbb{F}_q)|$. Many important enumeration results Cf. [2] can be realized by simply setting the indeterminants equal to 0 or 1. Using this idea, we give a concise and uniform mechanism (in the form of a small set of bivariate generating functions) for solving matrix enumeration problems. In particular we count

All $n\times n$ matrices over $\mathbb{F}_q$ classified by corank, Cf. A286331.

All $n\times n$ matrices over $\mathbb{F}_q$ classified by number of cyclic matrices in a cyclic decomposition, Cf. A346677

All $n\times n$ matrices over $\mathbb{F}_q$ classified by degree of minimal polynomial, Cf. A347010

Diagonalizable $n\times n$ matrices over $\mathbb{F}_q$ classified by corank, Cf A296548

Diagonalizable $n \times n$ matrices over $\mathbb{F}_q$ classified matrices by number of eigenvalues, Cf A296605

Triangularizable $n \times n$ matrices over $\mathbb{F}_q$ Cf. A346210

Idempotent $n \times n$ matrices over $\mathbb{F}_q$ classified by corank, Cf. A296548

Nilpotent $n \times n$ matrices over $\mathbb{F}_q$ classified by corank, Cf. A346412

Nilpotent $n \times n$ matrices over $\mathbb{F}_q$ classified by index, Cf. A346214

Cyclic $n \times n$ matrices over $\mathbb{F}_q$ classified by corank Cf. A346084

Cyclic $n \times n$ matrices over $\mathbb{F}_q$ classified by number of distinct irreducible factors

Indecomposable $n \times n$ matrices over $\mathbb{F}_q$
Semi-simple $n \times n$ matrices over $\mathbb{F}_q$ classified by number of distinct irreducible factors

Separable $n \times n$ matrices over $\mathbb{F}_q$ classified by number of distinct irreducible factors Cf. A344873

Simple $n \times n$ matrices over $\mathbb{F}_q$ Cf. A345463

Recurrent $n \times n$ matrices over $\mathbb{F}_q$ Cf. A348015

Preliminaries

Let Φ be the set of monic irreducible polynomials in $\mathbb{F}_q[z]$. Let $\phi \in \Phi$ with $\deg \phi = d$. Let $L = \{\emptyset, \{1\}, \{1,1\}, \{2\}, \{1,1,1\}, \{1,2\}, \{3\}, \{1,1,1,1\}, \ldots\}$ be the collection of all partitions of nonnegative integers taken as ordered multisets of positive integers where it is understood that the partition of the integer 0 is the empty set. Let $\lambda = \{\lambda_1 \leq \lambda_2 \leq \ldots \leq \lambda_j\} \in L$ with $\lambda_1 + \lambda_2 + \ldots + \lambda_j = |\lambda|$. Define $c_d(\lambda)$ to be the order of the group of module automorphisms of the $\mathbb{F}_q[z]$-module $\oplus_{i=1}^{j} \mathbb{F}_q[z]/\langle \phi^{\lambda_i} \rangle$. Equivalently, $c_d(\lambda)$ is the number of $d|\lambda| \times d|\lambda|$ invertible matrices that commute with A, where A is the direct sum of the companion matrices $C(\phi^{\lambda_1}), \ldots, C(\phi^{\lambda_j})$. In other words, A is the rational canonical form representative of the unique class of matrices having characteristic polynomial $\prod_{i=1}^{j} \phi^{\lambda_i} = \phi^{|\lambda|}$, minimal polynomial ϕ^{λ_j}, and invariant factor list: $\phi^{\lambda_1} | \phi^{\lambda_2} | \cdots | \phi^{\lambda_j}$. We see that

$c_d(\lambda)$ is also the order of the stabilizer subgroup of A under the action of conjugation by $GL_n(\mathbb{F}_q)$. So the size of the orbit of A under this action is $\frac{|GL_n(\mathbb{F}_q)|}{c_d(\lambda)}$. The following formula for the quantity $c_d(\lambda)$ is given in [1]

$$c_d(\lambda) = \prod_i \prod_{k=1}^{b_i} (q^{d \cdot s_i} - q^{(s_i - k)d})$$

where b_i is the number of parts in λ of size i and $s_i = 1 \cdot b_1 + 2 \cdot b_2 + \cdots + i \cdot b_i + i(b_{i+1} + \cdots + b_n)$.

Each conjugacy class in $\mathrm{Mat}_n(\mathbb{F}_q)$ is uniquely specified by the multiset of elementary divisors of a matrix in the class. So each class is determined by a function from Φ to L such that only finitely many values are nonempty. The finite set of ordered pairs $(\phi \in \Phi, \lambda \neq \emptyset \in L)$ given by such a function is called the conjugacy class data in [2].

Fix $l \subseteq L, d \geq 1$. Let length(λ) denote the number of its parts and max(λ) be the largest part where it is understood that length($\emptyset$) = 0 and max($\emptyset$) = 0. We define the following bivariate generating functions :

$$G_{d,l}(u,v) = \sum_{\lambda \in l} \frac{v^{\mathrm{length}(\lambda)} u^{d|\lambda|}}{c_d(\lambda)}$$

$$F_{d,l}(u,v) = \sum_{\lambda \in l} \frac{v^{\max(\lambda)} u^{d|\lambda|}}{c_d(\lambda)}$$

$$H_{d,l}(u,v) = \sum_{\lambda \in l} \frac{v u^{d|\lambda|}}{c_d(\lambda)} - v + 1$$

$$J_{d,l}(u,v) = \sum_{\lambda \in l} \frac{v^{d\max(\lambda)} u^{d|\lambda|}}{c_d(\lambda)}$$

These functions will be used in the following along with two important subsets of L defined below:

$$L_1 = \{\emptyset, \{1\}, \{1,1\}, \{1,1,1\}, \{1,1,1,1\}, \ldots\}$$

$$L_t = \{\emptyset, \{1\}, \{2\}, \{3\}, \{4\}, \ldots\}$$

Some classifications of all matrices in $Mat_n(\mathbb{F}_q)$

Let a_n be the total number of matrices in $\mathrm{Mat}_n(\mathbb{F}_q)$. Let ν_d be the number of monic irreducibles in Φ of degree d and let γ_n denote the order of $GL_n(\mathbb{F}_q)$. Then

$$\sum_{n\geq 0} \frac{a_n u^n}{\gamma_n} = \prod_{d\geq 1} (G_{d,L}(u,1))^{\nu_d}.$$

Let $a_{n,k}$ be the number of matrices T in $\mathrm{Mat}_n(\mathbb{F}_q)$ of corank k, $0 \leq k \leq n$. Note that the variable v in $G_{1,l}$ is counting $\dim(E(T,0))$ the dimension of the eigenspace corresponding to the eigenvalue 0. So we have:

$$\sum_{n\geq 0}\sum_{k=0}^{n} \frac{a_{n,k} v^k u^n}{\gamma_n} = G_{1,L}(u,v) \cdot (G_{1,L}(u,1))^{q-1} \cdot \prod_{d\geq 2} (G_{d,L}(u,1))^{\nu_d}$$

Let $a_{n,k}$ be the number of matrices T in $\mathrm{Mat}_n(\mathbb{F}_q)$ that can be decomposed into at most k cyclic matrices. Equivalently, $a_{n,k}$ is the number of matrices over the algebraic closure of $\mathbb{F}_q$ whose Jordan normal form has k blocks. Then

$$\sum_{n\geq 0}\sum_{k=0}^{n} \frac{a_{n,k} v^k u^n}{\gamma_n} = \prod_{d\geq 1} (G_{d,L}(u,v))^{\nu_d}$$

Let $a_{n,k}$ be the number of matrices T in $GL_n(\mathbb{F}_q)$ that can be decomposed into at most k cyclic matrices. Then $a_{n,k}$ is a q-analogue of the Stirling numbers of the first kind and we have:

$$\sum_{n\geq 0}\sum_{k=0}^{n} \frac{a_{n,k} v^k u^n}{\gamma_n} = (G_{d,L}(u,v))^{q-1} \prod_{d\geq 2} (G_{d,L}(u,v))^{\nu_d}$$

Let $a_{n,k}$ be the number of matrices T in $\mathrm{Mat}_n(\mathbb{F}_q)$ that have minimal polynomial of degree k. The variable v in $J_{d,l}(u,v)$ is counting the degree of each irreducible factor in the minimal polynomial. So we have:

$$\sum_{n\geq 0}\sum_{k=0}^{n} \frac{a_{n,k} v^k u^n}{\gamma_n} = \prod_{d\geq 1} (J_{d,L}(u,v))^{\nu_d}$$

Diagonalizable matrices

A matrix T in $\mathrm{Mat}_n(\mathbb{F}_q)$ is diagonalizable if and only if $\sum_{a\in\mathbb{F}_q}\dim(E(T,a))=n$. Equivalently, the conjugacy class data for a diagonalizable matrix T contains only linear polynomials paired with partitions of the form $\{1\le 1\le\cdots\le 1\}$. Now let L_1 be the set of all such partitions along with $\emptyset$. Let a_n be the number of diagonalizable matrices in $\mathrm{Mat}_n(\mathbb{F}_q)$. Then

$$\sum_{n\ge 0}\frac{a_n u^n}{\gamma_n}=(G_{1,L_1}(u,1))^q.$$

Let $a_{n,k}$ be the number of diagonalizable matrices in $\mathrm{Mat}_n(\mathbb{F}_q)$ of corank $k,\ 0\le k\le n$. Then

$$\sum_{n\ge 0}\sum_{k=0}^{n}\frac{a_{n,k}v^k u^n}{\gamma_n}=G_{1,L_1}(u,v)\cdot(G_{1,L_1}(u,1))^{q-1}.$$

Let $a_{n,k}$ be the number of diagonalizable matrices in $\mathrm{Mat}_n(\mathbb{F}_q)$ having k distinct eigenvaules $0\le k\le q$. Then

$$\sum_{n\ge 0}\sum_{k=0}^{n}\frac{a_{n,k}v^k u^n}{\gamma_n}=(H_{1,L_1}(u,v))^q.$$

Triangularizable matrices

A matrix T in $\mathrm{Mat}_n(\mathbb{F}_q)$ is triangularlizable if it is similar to an upper triangular matrix. In other words, if there is a basis $b_1,\ldots,b_n$ for $\mathbb{F}_q^n$ such that $Tb_i\in\langle b_1,\ldots,b_i\rangle$ for all $1\le i\le n$. It is shown in [3] that a matrix T is triangularizable if and only if μ_T splits (its factorization contains only powers of linear polynomials). Let a_n be the number of triangularizable matrices in $\mathrm{Mat}_n(\mathbb{F}_q)$. Then

$$\sum_{n\ge 0}\frac{a_n u^n}{\gamma_n}=(G_{1,L}(u,1))^q.$$

Idempotent matrices

A matrix T is idempotent (a projection) if $T^2 = T$. Equivalently, if it is diagonalizable and has only eigenvalues of 0 or 1. Accordingly, the conjugacy class data contains only pairs with polynomials z or $z-1$ and partitions of the form $1 \leq 1 \leq \cdots \leq 1$. Let a_n be the number of idempotent matrices in $\mathrm{Mat}_n(\mathbb{F}_q)$. Then

$$\sum_{n\geq 0} \frac{a_n u^n}{\gamma_n} = (G_{1,L_1}(u,1))^2.$$

Let $a_{n,k}$ be the number of idempotent matrices in $\mathrm{Mat}_n(\mathbb{F}_q)$ of corank k, $0 \leq k \leq n$. Then

$$\sum_{n\geq 0}\sum_{k=0}^{n} \frac{a_{n,k} v^k u^n}{\gamma_n} = G_{1,L_1}(u,v) \cdot G_{1,L_1}(u,1).$$

Nilpotent matrices

A nilpotent matrix is a matrix T such that $T^m = 0$ for some positive integer m. The least such m is called the index of T. A matrix $T \in \mathrm{Mat}_n(\mathbb{F}_q)$ is nilpotent if and only if the characteristic polynomial $\mathcal{X}(z) = z^n$. The conjugacy class data contains only the polynomial z paired with any partition. Let a_n be the number of nilpotent matrices in $\mathrm{Mat}_n(\mathbb{F}_q)$. Then

$$\sum_{n\geq 0} \frac{a_n u^n}{\gamma_n} = G_{1,L}(u,1).$$

Let $a_{n,k}$ be the number of nilpotent matrices in $\mathrm{Mat}_n(\mathbb{F}_q)$ of corank k, $0 \leq k \leq n$. Then

$$\sum_{n\geq 0}\sum_{k=0}^{n} \frac{a_{n,k} v^k u^n}{\gamma_n} = G_{1,L}(u,v).$$

Let $a_{n,m}$ be the number of nilpotent matrices in $\mathrm{Mat}_n(\mathbb{F}_q)$ with index $m,\ 1 \leq m \leq n$. Then

$$\sum_{n\geq 0}\sum_{m=0}^{n}\frac{a_{n,m}v^m u^n}{\gamma_n} = F_{1,L}(u,v).$$

Cyclic matrices

A matrix $T \in \mathrm{Mat}_n(\mathbb{F}_q)$ is cyclic if there is a vector v such that $\mathrm{span}(\{T^i v : i \geq 0\}) = \mathbb{F}_q^n$. The minimal polynomial $\mu_T(z)$ is a proper divisor of $\mathcal{X}_T(z)$ if and only if for every $v \in \mathbb{F}_q^n,\ \mathrm{span}(\{T^i v : i \geq 0\})$ is a proper subspace of $\mathbb{F}_q^n$. In other words, T is cyclic if and only if $\mu_T(z) = \mathcal{X}_T(z)$. The subspace lattice of these matrices is isomorphic to a cross product of chains. The conjugacy class data will contain only trivial partitions. Let L_t be the set of such partitions along with $\emptyset$. Let a_n be the number of cyclic matrices in $\mathrm{Mat}_n(\mathbb{F}_q)$. Then

$$\sum_{n\geq 0}\frac{a_n u^n}{\gamma_n} = \prod_{d\geq 1}(G_{d,L_t}(u,1))^{\nu_d}.$$

Owing to the constraint on the partitions in the conjugacy class data we see that $\dim(E(T,a))$ is 0 or 1 for every $a \in \mathbb{F}_q$ so that the corank of any cyclic matrix is either 0 or 1. Let $a_{n,k}$ be the number of cyclic matrices in $\mathrm{Mat}_n(\mathbb{F}_q)$ with corank $k,\ 0 \leq k \leq 1$. Then

$$\sum_{n\geq 0}\sum_{k=0}^{1}\frac{a_{n,k}v^k u^n}{\gamma_n} = G_{1,L_t}(u,v)\cdot(G_{1,L_t}(u,1))^{q-1}\cdot\prod_{d\geq 2}(G_{d,L_t}(u,1))^{\nu_d}$$

Let $a_{n,k}$ be the number of cyclic matrices in $\mathrm{Mat}_n(\mathbb{F}_q)$ with k distinct irreducible polynomials in its factorization. These matrices have subspace lattices isomorphic to a crossproduct of k chains. We have

$$\sum_{n\geq 0}\sum_{k=0}^{n}\frac{a_{n,k}v^k u^n}{\gamma_n} = \prod_{d\geq 1}H_{d,L_t}(u,v).$$

Indecomposable matrices

Call a matrix is indecomposable if and only if it is cyclic and its minimal polynomial is the power of a single irreducible. These matrices have invariant subspace lattices that are chains. The conjugacy class data contains only one irreducible polynomial paired with a trivial partition. Then the number of indecomposable matrices in $\mathrm{Mat}_n(\mathbb{F}_q)$ is the coefficient of $\frac{vu^n}{\gamma_n}$ in the expansion of the above generating function.

Semi-simple matrices

A matrix $T \in \mathrm{Mat}_n(\mathbb{F}_q)$ is semi-simple if it is diagonalizable over the algebraic closure of $\mathbb{F}_q$. This means that $\mu_T(z)$ must be square free. The conjugacy class data contains only partitions of the form $1 \leq 1 \leq \cdots \leq 1$. Let a_n be the number of semi-simple matrices in $\mathrm{Mat}_n(\mathbb{F}_q)$. Then

$$\sum_{n\geq 0} \frac{a_n u^n}{\gamma_n} = \prod_{d\geq 1} (G_{d,L_1}(u,1))^{\nu_d}.$$

Let $a_{n,k}$ be the number of semi-simple matrices in $\mathrm{Mat}_n(\mathbb{F}_q)$ whose minimal polynomial is the product of k distinct irreducible factors. Then

$$\sum_{n\geq 0}\sum_{k} \frac{a_{n,k} v^k u^n}{\gamma_n} = \prod_{d\geq 1} (H_{d,L_1}(u,v))^{\nu_d}$$

Separable matrices

Call a matrix $T \in \mathrm{Mat}_n(\mathbb{F}_q)$ separable if it is both semi-simple and cyclic. These matrices are characterized by having squarefree characteristic polynomials. So the invariant subspace lattice of these matrices is isomporphic to the Boolean lattice. The only partitions in the conjugacy class data are empty and $\{1\}$ which is the intersection of L_1 and L_t. Let a_n be the number of separable matrices in $\mathrm{Mat}_n(\mathbb{F}_q)$. Then

$$\sum_{n\geq 0} \frac{a_n u^n}{\gamma_n} = \prod_{d\geq 1} (G_{d,L_1\cap L_t}(u,1))^{\nu_d}.$$

Let $a_{n,k}$ be the number of separable matrices in $\mathrm{Mat}_n(\mathbb{F}_q)$ whose characteristic polynomial is the product of k distinct irreducible factors. Equivalently, $a_{n,k}$ is the number of matrices in $\mathrm{Mat}_n(\mathbb{F}_q)$ whose invariant subspace lattice is isomorphic to the Boolean lattice $\mathbf{B}_k$. Then

$$\sum_{n\geq 0}\sum_{k}\frac{a_{n,k}v^k u^n}{\gamma_n}=\prod_{d\geq 1}(H_{d,L_1\cap L_t}(u,v))^{\nu_d}$$

Simple matrices

Call a matrix $T\in \mathrm{Mat}_n(\mathbb{F}_q)$ simple if there are no nontrivial T-invariant subspaces. Equivalently, every nonzero vector in $\mathbb{F}_q^n$ is a cyclic vector, i.e., for each nonzero vector $v\in\mathbb{F}_q^n$, $\mathrm{span}(\{T^i v : i\geq 0\})=\mathbb{F}_q^n$. It must be that $\mathcal{X}_T(z)=\mu_T(z)$ is irreducible. So the conjugacy class data contains only irreducible polynomials paired with the empty partition or $\{1\}$. Then the number of simple matrices in $\mathrm{Mat}_n(\mathbb{F}_q)$ is the coefficient of $\frac{vu^n}{\gamma_n}$ in the expansion of the above generating function.

Recurrent matrices

Call a matrix $T\in \mathrm{Mat}_n(\mathbb{F}_q)$ recurrent if $T=T^k$ for some $k>1$. Then T is recurrent if and only if $\mathrm{im}T=\mathrm{im}T^2$ if and only if z^2 does not divide $m_T(z)$, the minimal polynomial of T. Let a_n be the number of recurrent matrices in $\mathrm{Mat}_n(\mathbb{F}_q)$. Then

$$\sum_{n\geq 0}\frac{a_n u^n}{\gamma_n}=G_{1,L_1}(u,1,)G_{1,L}(u,1)\prod_{d\geq 2}(G_{d,L}(u,1))^{\nu_d}.$$

Order of invertible matrices

The order of a matrix $T\in GL_n(\mathbb{F}_q)$ is the smallest positive integer k such that $T^k=I$. Let $\mu_T(z)$ be the minimal polynomial of T. Then the order of T is the smallest positive integer k so that $\mu_T(z)|z^k-1$. Suppose the order of T divides m. Let $z^m-1=\phi_1^e\phi_2^e\cdots\phi_j^e$ with $\deg(\phi_i)=d_i$. The conjugacy class data contains only the irreducible polynomials ϕ_i and the partitions of integers into parts of size at most e. Let L_e be the set of such partitions along with $\emptyset$. Let a_n be the number of matrices in $\mathrm{Mat}_n(\mathbb{F}_q)$ whose order divides m. Then

$$\sum_{n\geq 0}\frac{a_n u^n}{\gamma_n}=\prod_{i}(G_{d_i,L_e}(u,1)).$$

References

[1] Joseph Kung, The cycle structure of a linear transformation over a finite field, *Linear Algebra and its Applications*, **36** (1981). 141-155.

[2] Kent Morrison, Integer sequences and matrices over finite fields, *Journal of Integer Sequences*, **9** (2006) , Article 06.2.1.

[3] Pete Clark, Linear Algebra: Invariant Subspaces (UGA Math).