COUNTING MATRICES OVER FINITE FIELDS

GEOFFREY CRITZER

ABSTRACT. In this expository piece we give a reckoning of $\mathrm{Mat}_n(\mathbb{F}_q)$, the ring of $n \times n$ matrices over the field $\mathbb{F}_q$, containing q elements. In Section 1 we give relevant definitions and describe some concepts necessary for an understanding of the structure of $\mathrm{Mat}_n(\mathbb{F}_q)$. In Section 2 we give an interpretation of the elements in a binomial poset which, in accordance with the theory of binomial posets (Cf. [1],[2]), explains the ubiquitous appearance of generating functions of the form $\sum_{n\geq 0} a_n \frac{u^n}{\gamma_n}$ where a_n denotes the size of some desired class of $n \times n$ matrices and $\gamma_n = |GL_n(\mathbb{F}_q)|$. In Section 3 we employ the cycle index for conjugation action of $GL_n(\mathbb{F}_q)$ on $\mathrm{Mat}_n(\mathbb{F}_q)$ to derive bivariate generating functions counting many classes of matrices conditioned by various parameters. In the final section we derive explicit formulas for the size and number of torsion classes in $\mathrm{Mat}_n(\mathbb{F}_q)$. We also give an asymptotic limit for the probability that a matrix is periodic.

1. $\mathbb{F}_q[x]$-MODULES AND CANONICAL FORMS

In this section, for $A \in \mathrm{Mat}_n(\mathbb{F}_q)$ we define the corresponding $\mathbb{F}_q[x]$-module, M^A on the vector space $\mathbb{F}_q^n$. We define the rational canonical form for a matrix as well as a primary rational canonical form. We use techniques demonstrated in [3],[4] to deduce the generating function $C_q(u)$ counting the number of conjugacy classes of $n \times n$ matrices over $\mathbb{F}_q$. A slight variation of this function gives the number of conjugacy classes in the general linear group $GL_n(\mathbb{F}_q)$. We show that $C_q(u)$ also counts the number of integer partitions of n into parts that are colored with at most q colors. In like manner we count the number of cyclic matrices.

Let T be a linear transformation on an n-dimensional vector space V over a finite field $\mathbb{F}_q$. Let $\mathcal{V} = \{\vec{v_1}, \vec{v_2}, \ldots, \vec{v_n}\}$ be a basis of V. The map T is completely determined by its values on $\mathcal{V}$ so T can be encoded in an $n \times n$ *transformation matrix* A whose i^{th} column is the vector $(a_1, \ldots, a_n)^t$ where $T(\vec{v_i}) = a_1\vec{v_1} + \cdots + a_n\vec{v_n}$. There are of course q^{n^2} matrices in $\mathrm{Mat}_n(\mathbb{F}_q)$. It is natural to identify those matrices which are the transformation matrices of the same linear transformation but with respect to different bases. This identification, an equivalence relation on $\mathrm{Mat}_n(\mathbb{F}_q)$, is made precise in the following definition.

Definition 1.1. Two $n \times n$ matrices A and B are *similar* if there is a matrix P such that $B = P^{-1}AP$.

2020 *Mathematics Subject Classification.* Primary: 13D02, 13H10. Secondary: 14B99.

Example: Let V be the 4-dimensional vector space of polynomials in $\mathbb{F}_2[x]$ of degree at most 3. Let $\mathcal{V} = \langle 1, x, x^2, x^3 \rangle$, $\mathcal{P} = \langle 1, x, x^2 + x, x^3 + x^2 \rangle$ be bases of V. Let $T \in \mathcal{L}(V)$ be the derivative operator: $T(\sum_{i=0}^{3} a_i x^i) = \sum_{i=1}^{3} i \cdot a_i x^{i-1}$ where each $a_i \in \mathbb{F}_2$.

$$A = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$ is the transformation matrix of T with respect to $\mathcal{V}$

$$B = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$ is the transformation matrix of T with respect to $\mathcal{P}$

$$P = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$ is the matrix whose i^{th} column is the coordinate vector of $\vec{p_i}$ with respect to $\mathcal{V}$ where $\vec{p_i}$ is the i^{th} basis vector of $\mathcal{P}$.

We see that A and B are distinct matrices that represent the same linear operator and $B = P^{-1}AP$.

Given an $n \times n$ matrix A with entries in $\mathbb{F}_q$, we can define an $\mathbb{F}_q[x]$ module M^A by $f(x) * \vec{v} = f(A)\vec{v}$ for all $\vec{v} \in \mathbb{F}_q^n$ and for all $f(x) \in \mathbb{F}_q[x]$.

Two matrices A and B are similar if and only if $M^A \cong M^B$. So the number of conjugacy classes of $n \times n$ matrices over $\mathbb{F}_q$ is equal to the number of non-isomorphic $\mathbb{F}_q[x]$ modules M^A which is equal to the number of distinct linear operators on $\mathbb{F}_q^n$.

From the structure theorem of finitely generated modules over a principal ideal domain (C.f. [5]) we have two important decompositions of the module M^A into cyclic submodules: the *invariant factor decomposition* and the *primary decomposition*. The invariant factor decomposition is shown below.

$$M^A \cong \mathbb{F}_q[x]/\langle a_1(x) \rangle \oplus \mathbb{F}_q[x]/\langle a_2(x) \rangle \oplus \cdots \oplus \mathbb{F}_q[x]/\langle a_k(x) \rangle$$

The $a_i(x) \in \mathbb{F}_q[x]$ are unique up to multiplication by a unit so we may as well assume that they are monic. They form the (ordered by divisibility) *list of invariant factors* of

the matrix A. In other words, $a_1(x)|a_2(x)|\cdots|a_k(x)$ where $a_k(x)$ is the minimal polynomial $\mu_A(x)$ of A and $\prod_{i=1}^{k} a_i(x)$ is the characteristic polynomial $\chi_A(x)$ of A.

In the primary decompostion, the *elementary divisors* are powers of a monic irreducible (prime) polynomial in $\mathbb{F}_q[x]$. The primary decomposition is unique up to ordering of the factors.

$$M^A \cong \oplus_{i=1}^{k} \oplus_{j=1}^{l_i} \mathbb{F}_q[x]/\langle \phi_i(x)^{\lambda_{i,j}} \rangle$$

where k is the number of distinct primes in the factorization of $\chi(x)$ and for each i, $\lambda_{i,1} \geq \lambda_{i,2} \geq \ldots \geq \lambda_{i,l_i}$ is a partition of n_i, the multiplicity of ϕ_i in $\chi_A(x)$. In other words, n_i is the exponent of ϕ_i in the prime factorization of $\chi_A(x)$ so that $\sum_{i=1}^{k} deg\phi_i \cdot n_i = n$.

The *rational canonical form* RCF of a matrix A is the block diagonal matrix whose blocks are the companion matrices of the invariant factors of M^A. Each such matrix is the unique (canonical) representative of a distinct conjugacy class. In other words, the number of distinct rational canonical forms of an $n \times n$ matrix over $\mathbb{F}_q$ is equal to the number of distinct linear operators on $\mathbb{F}_q^n$.

The *primary rational canonical form* PRCF of a matrix A is the block diagonal matrix whose blocks are the companion matrices of the elementary divisors of M^A. If we agree on how to order the elementary divisors then we can consider each such matrix as a canonical representative of its conjugacy class.

We note that it is not always the case that the invariant factors are distinct from the elementary divisors. In fact, equality of the two forms happens precisely when $\chi_A(x)$ is of the form $\phi(x)^m$ for some monic irreducible $\phi(x)$ and positive integer m. In Section 3 we enumerate all such matrices (which are called *primary matrices*). It is also important to realize that neither of these two forms are equivalent to the Jordan canonical form even when the characteristic polynomial splits into linear factors in $\mathbb{F}_q[x]$.

The number of conjugacy classes.

Constructing the multiset of elementary divisors corresponding to a matrix A amounts to choosing nonconstant monic irreducibile polynomials $\phi_1(x), \ldots, \phi_k(x) \in \mathbb{F}_q[x]$ and to each $\phi_i(x)$ associating a partition λ_i of a positive integer n_i. This association is called the *conjugacy class data* by Morrison in [4]. In Section III we will use it to define the *cycle index for matrices.*

Let p_n be the number of partitions of integer n.

$$\sum_{n>=0} p_n u^n = \prod_{i \geq 1} \frac{1}{1-u^i} = 1 + u + 2u^2 + 3u^3 + 5u^4 + \cdots$$

Let $c_{n,q}$ be the number of conjugacy classes in $\mathrm{Mat}_n(\mathbb{F}_q)$. Let $\nu_q(j)$ be the number of monic irreducible polynomials in $\mathbb{F}_q[x]$ of degree j. In [6] it is shown that $\nu_q(n) = \frac{1}{n}\sum_{d|n}\mu(\frac{n}{d})q^d$ (a result attributed to C. F. Gauss). Let $C_q(u)$ be the generating function for the number of conjugacy classes in $\mathrm{Mat}_n(\mathbb{F}_q)$.

$$C_q(u) = \sum_{n=0}^{\infty} c_{n,q}u^n =$$

$(1+u+2u^2+3u^3+5u^4+\cdots)^{\nu_q(1)}(1+u^2+2(u^2)^2+3(u^2)^3+5(u^2)^4+\cdots)^{\nu_q(2)}(1+u^3+2(u^3)^2+3(u^3)^3+5(u^3)^4+\cdots)^{\nu_q(3)}\cdots =$

$\prod_{j\geq 1}\prod_{i\geq 1}(\frac{1}{1-u^{ij}})^{\nu_q(j)}$

Example: The case for $q = 2$.

Note that $\nu_2(1) = 2, \nu_2(2) = 1, \nu_2(3) = 2\ldots$ (because the monic irreducibles in $\mathbb{F}_2[x]$ are: $x, x+1, x^2+x+1, x^3+x+1, x^3+x^2+1\ldots$). In the expansion of $C_2(u)$ below, the coefficients of the terms are the partition numbers. A typical contribution to the coefficient of x^6 in the expansion of $C_2(u)$ is the product of the boldface terms indicated below.

$(1+\mathbf{u}+2u^2+3u^3+5u^4+\cdots)(1+\mathbf{u}+2u^2+3u^3+5u^4+\cdots)$
$(1+u^2+\mathbf{2u^4}+3u^6+5u^8+\cdots)$
$(\mathbf{1}+u^3+2u^6+3u^9+5u^{12}+\cdots)(\mathbf{1}+u^3+2u^6+3u^9+5u^{12}+\cdots)$
$(\mathbf{1}+\cdots)(\mathbf{1}+\cdots)(\mathbf{1}+\cdots)\ldots$

The indicated product $2u^6$ corresponds to the 2 conjugacy classes of 6×6 matrices over $\mathbb{F}_2$ whose characteristic polynomial is $\chi(x) = x(x+1)(x^2+x+1)^2$. There are 2 lists of invariant factors because there are 2 partitions of the exponent two of the right most factor of $\chi(x)$:

$$x(x+1)(x^2+x+1)^2 \text{ corresponds to the partition 2.}$$

$$x^2+x+1 \mid x(x+1)(x^2+x+1) \text{ corresponds to the partition 1+1.}$$

Note that we have left the invariant factors in their factored form for clarity. The first invariant factor list contains only a single member so that the matrices in this class are precisely those whose minimal polynomial equals the characteristic polynomial equals $x(x+$

$1)(x^2+x+1)^2$. The rational canonical form of these matrices is the companion matrix of $\chi(x) = x(x+1)(x^2+x+1)^2 = x^6+x^5+x^4+x^3+x^2+x$. The blocks of the primary rational canonical form are the elementary divisors $x, x+1, (x^2+x+1)^2$. Note that $(x^2+x+1)^2 = x^4+x^2+1$

$$\text{RCF}\begin{pmatrix} 0&0&0&0&0&0\\ 1&0&0&0&0&1\\ 0&1&0&0&0&1\\ 0&0&1&0&0&1\\ 0&0&0&1&0&1\\ 0&0&0&0&1&1 \end{pmatrix} \sim PRCF\begin{pmatrix} 0&0&0&0&0&0\\ 0&1&0&0&0&0\\ 0&0&0&0&0&1\\ 0&0&1&0&0&0\\ 0&0&0&1&0&1\\ 0&0&0&0&1&0 \end{pmatrix}$$

The matrices specified by the second list of invariant factors have minimal polynomial $x(x+1)(x^2+x+1) = x^4+x$. The rational canonical form of these matrices is composed of two blocks corresponding to the companion matrices of x^2+x+1 and x^4+x. The multiset of elementary divisors contains: $x, x+1, x^2+x+1, x^2+x+1$ so that the blocks of the primary rational canonical form are the corresponding companion matrices.

$$RCF\begin{pmatrix} 0&1&0&0&0&0\\ 1&1&0&0&0&0\\ 0&0&0&0&0&0\\ 0&0&1&0&0&1\\ 0&0&0&1&0&0\\ 0&0&0&0&1&0 \end{pmatrix} \sim PRCF\begin{pmatrix} 0&0&0&0&0&0\\ 0&1&0&0&0&0\\ 0&0&0&1&0&0\\ 0&0&1&1&0&0\\ 0&0&0&0&0&1\\ 0&0&0&0&1&1 \end{pmatrix}$$

Having the generating function $C_q(u)$, it is straight forward to count the number of conjugacy classes in $GL_n(\mathbb{F}_q)$. A matrix is invertible if and only if it does not have 0 as an eigenvalue if and only if x does not divide its characteristic polynomial. We just need to omit the factor corresponding to the monic irreducible x in our generating function for $C_q(u)$. Let $a_{n,q}$ be the number of conjugacy classes of the general linear group $GL_n(\mathbb{F}_q)$.

$$\sum_{n=0}^{\infty} a_{n,q}x^n = (\frac{1}{1-u})^{\nu_q(1)-1}\prod_{j\geq 2}\prod_{i\geq 1}(\frac{1}{1-u^{ij}})^{\nu_q(j)} = C_q(u)\prod_{i\geq 1}(1-u^i)$$

For the case $q=2$ the terms of $a_{n,2}$ are given in sequence A006951. For $n = 0, 1, \ldots 10$ we have:

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

Number of partitions with colored parts

In [6] it is also shown that since each of the q^n monic polynomials in $\mathbb{F}_q[x]$ has a unique factorization into monic irreducible polynomials, we have:

$$\frac{1}{1-qu} = \prod_{j\geq 1}(\frac{1}{1-u^j})^{\nu_q(j)}.$$

Following [4] we make the substitution $u \to u^i$ to obtain:

$$\frac{1}{1-qu^i} = \prod_{j\geq 1}(\frac{1}{1-u^{ij}})^{\nu_q(j)}.$$

So we can rewrite our expression for $C_q(u)$

$$C_q(u) = \prod_{j\geq 1}\prod_{i\geq 1}(\frac{1}{1-u^{ij}})^{\nu_q(j)}$$

$$= \prod_{i\geq 1}\prod_{j\geq 1}(\frac{1}{1-u^{ij}})^{\nu_q(j)}$$

$$= \prod_{i\geq 1}\frac{1}{1-qu^i}$$

Viewing q as a variable, the last expression is the bivariate generating function for the number of integer partitions classified by number of parts. Then taking q as a constant, $C_q(u)$ counts the number of integer partitions where we have q choices for the type (or color) of each part in the partition.

Number of cyclic matrices

A matrix is cyclic if and only if its characteristic polynomial is equal to its minimal polynomial. For each monic polynomial $p(x)$ in $\mathbb{F}_q[x]$ with degree n there is exactly one similarity class of matrices in $M_n(\mathbb{F}_q)$ whose members have $p(x)$ as both their characteristic polynomial and their minimal polynomial. We want to count the number of matrices in each of these q^n classes.

Let $A \in \mathrm{Mat}_n(\mathbb{F}_q)$ with characteristic polynomial = $p(x)$ = minimal polynomial. Let $[A]$ be the class of matrices similar to A. Each such class $[A]$ corresponds to a cyclic $\mathbb{F}_q[x]$ module M^A. Let $\vec{v}$ be a cyclic vector in M^A. Then the annhilator $I_v := \{f(x) \in \mathbb{F}_q[x] : f(x)\vec{v} = \vec{0}\} = \langle p(x)\rangle$ and $M^A \cong \mathbb{F}_q[x]/\langle p(x)\rangle$.

We will count the number of automorphisms of the ring $\mathbb{F}_q[x]/\langle p(x)\rangle$. Let $p(x) = p_1(x)^{e_1}p_2(x)^{e_2}\dots p_k(x)^{e_k}$ where each $p_i(x)$ is a distinct irreducible polynomial in $\mathbb{F}_q[x]$. Then $\mathbb{F}_q[x]/\langle p(x)\rangle \cong \mathbb{F}_q[x]/\langle p_1(x)^{e_1}\rangle \times \mathbb{F}_q[x]/\langle p_1(x)^{e_2}\rangle \times \cdots \times \mathbb{F}_q[x]/\langle p_1(x)^{e_k}\rangle$. So it suffices to count the automorphisms of $\mathbb{F}_q[x]/\langle a(x)^e\rangle$ where $a(x)$ is irreducible in $\mathbb{F}_q[x]$.

From [7] we have that the number of units in the ring $\mathbb{F}_q[x]/\langle a(x)^e\rangle$ is given by the generalized Euler phi function for polynomials: $\Phi(a(x)^e) = (c-1)c^{e-1}$ where c is the cardinality of (the field) $\mathbb{F}_q[x]/\langle a(x)\rangle$. So there are $\Phi(a(x)^e)$ generators in our ring $\mathbb{F}_q[x]/\langle a(x)^e\rangle$. Any automorphism maps this set of generators to itself and is completely determined by the choice of the image of (say) the generator 1. So there are exactly $\Phi(a(x)^e)$ automorphisms of $\mathbb{F}_q[x]/\langle a(x)^e\rangle$.

Example: Let $q = 2, n = 4, A = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}$.

The matrix A is in rational canonical form and consists of a single block. So we have that the characteristic polynomial = minimal polynomial $= 1+x+x^3+x^4 = (1+x)^2(1+x+x^2)$. So there are $\Phi((1+x)^2)\cdot\Phi(1+x+x^2) = 2\cdot 3 = 6$ automorphisms of M^A:

$$\begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 \end{pmatrix},$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix}$$

We can read the generators from the (A-cyclic) vectors in the first column of each matrix to obtain the 6 units in the ring:

$$x,\ x^2,\ x^3,\ 1,\ 1+x^2+x^3,\ 1+x+x^3$$

These are precisely the polynomials in $\mathbb{F}_2[x]$ of degree less than 4 that are relatively prime to $1+x+x^3+x^4$.

Finally, the number of matrices that are similar to A is $\frac{|GL_4(\mathbb{F}_2)|}{6} = 3360$.

In order to tally up the number of similar matrices in each class we can use the same idea for a generating function as we used to count conjugacy classes above. This time we replace the partition numbers with the (multiplicative inverses of) values of the Φ function.

Let $b_{n,q} = b_n$ be the number of $n \times n$ cyclic matrices over $\mathbb{F}_q$. Let $\gamma_{n,q} = \gamma_n = |GL_n(\mathbb{F}_q)|$. Let $\nu_{d,q} = \nu_d$ be the number of monic irreducible polynomials of degree d over $\mathbb{F}_q$. Let $a_{d,q}(x) = a_d(x)$ be any degree d monic irreducible in $\mathbb{F}_q[x]$. Then observing that Φ is multiplicative we have:

$$\sum_{n\geq 0} b_n \frac{x^n}{\gamma_n} =$$

$$\begin{gathered}(1 + \tfrac{1}{\Phi(a_1(x))}x + \tfrac{1}{\Phi(a_1(x)^2)}x^2 + \tfrac{1}{\Phi(a_1(x)^3)}x^3 + \cdots)^{\nu_1} \\ (1 + \tfrac{1}{\Phi(a_2(x))}x^2 + \tfrac{1}{\Phi(a_2(x)^2)}x^4 + \tfrac{1}{\Phi(a_2(x)^3)}x^6 + \cdots)^{\nu_2} \\ (1 + \tfrac{1}{\Phi(a_3(x))}x^3 + \tfrac{1}{\Phi(a_3(x)^2)}x^6 + \tfrac{1}{\Phi(a_3(x)^3)}x^9 + \cdots)^{\nu_3} \cdots\end{gathered}$$

For all $d, e \geq 1$, $\Phi((a_d(x)^e) = (q^d - 1)(q^d)^{e-1}$ so the equation becomes

$$\sum_{n\geq 0} b_n \frac{x^n}{\gamma_n} = \prod_{d\geq 1}(1 + \sum_{e\geq 1} \frac{1}{(q^d - 1)(q^d)^{e-1}}x^{de})^{\nu_d}$$

Recognizing the sum as a geometric series the RHS simplifies to

$$\sum_{n\geq 0} b_n \frac{x^n}{\gamma_n} = \prod_{d\geq 1}(1 + \frac{1}{q^d - 1}\frac{x^d}{1 - (\frac{x}{q})^d})^{\nu_d}$$

The case for $q = 2$ is the sequence A346082. The first few terms indexed from $n = 0$ are:

1, 2, 14, 412, 50832, 25517184, 51759986688, 422000664182784, ...

A matrix is invertible if and only if its characteristic polynomial $f(x)$ is not divisble by x. The number of invertible cyclic matrices can be found by decrementing the exponent ν_1 in our generating function by 1. Let $r_{n,q} = r_n$ be the number of such matrices. Then we have:

$$\sum_{n\geq 0} r_n \frac{x^n}{\gamma_n} =$$

$$\begin{gathered}(1+\tfrac{1}{\Phi(a_1(x))}x+\tfrac{1}{\Phi(a_1(x)^2)}x^2+\tfrac{1}{\Phi(a_1(x)^3)}x^3+\cdots)^{\nu_1-1}\\ (1+\tfrac{1}{\Phi(a_2(x))}x^2+\tfrac{1}{\Phi(a_2(x)^2)}x^4+\tfrac{1}{\Phi(a_2(x)^3)}x^6+\cdots)^{\nu_2}\\ (1+\tfrac{1}{\Phi(a_3(x))}x^3+\tfrac{1}{\Phi(a_3(x)^2)}x^6+\tfrac{1}{\Phi(a_3(x)^3)}x^9+\cdots)^{\nu_3}\cdots =\end{gathered}$$

$$(1+\tfrac{1}{q-1}\tfrac{x}{1-(\frac{x}{q})})^{\nu_1-1}\prod_{d\geq 2}(1+\tfrac{1}{q^d-1}\tfrac{x^d}{1-(\frac{x}{q})^d})^{\nu_d}$$

For the case $q=2$ this is sequence A346084.

1, 1, 5, 146, 17352, 8607552, 17362252800, 141087882903552, ...

We note that in the case that a matrix is cyclic, the determination of the number of module automorphisms is easy. This is not the case generally. In Section 3 we will see a remarkable formula due to Joseph Kung [13] counting the number of module automorphisms. We will use this formula to derive the cycle index for matrices.

2. The binomial poset $\mathcal{E}$ of idempotent matrices over $\mathbb{F}_q$

The theory of binomial posets is an attempt to explain why some forms of generating functions (e.g. ordinary, exponential, Eulerian, Dirichlet,...) appear frequently in combinatorial enumeration problems [1,2,20,21] . Binomial posets provide a mechanical means of deriving generating functions for the combinatorial classes of their elements.

In this section we define a poset $\mathcal{E}_n$ on the set of $n\times n$ idempotent matrices over $\mathbb{F}_q$. We show that $\mathcal{E}_n$ is isomorphic to a typical n-interval in the binomial poset $\mathcal{E}$ of all infinite idempotent matrices over $\mathbb{F}_q$ having only finitely many nonzero entries. We show that $\mathcal{E}$ has factorial function $B(n)=\frac{\gamma_n}{(q-1)^n}$ where $\gamma_n=|\mathrm{GL}_n(\mathbb{F}_q)|$. For any $E\in\mathcal{E}_n$, let C_E be the set of saturated chains in $\mathcal{E}_n$ from $\hat{0}$ to E. We give a many-to-one correspondence between C_E and the elements in G_E the maximal subroup (of the semigroup $\mathrm{Mat}_n(\mathbb{F}_q)$) containing E. We derive generating functions corresponding to some important functions in $R(\mathcal{E})$ the reduced incidence algebra of the binomial poset $\mathcal{E}$.

The following definition is given in [8].

Definition 2.1. A poset P is a *binomial poset* if it satisfies the following 3 conditions

i) P is locally finite (i.e. every interval is finite) with $\hat{0}$ and contains an infinite chain.
ii) Every interval $[s,t]$ of P is graded (i.e. every maximal chain in $[s,t]$ has the same length). If the length of interval $[s,t]$ is n then we call it an n-interval.
iii) For all $n \geq 0$, any two n-intervals contain the same number of maximal chains. The number of maximal chains in an n-interval is denoted $B(n)$ and is called the *factorial function* of P.

Example: The following familiar posets satisfy the above conditions:

The poset of positive integers $\mathbb{P}$ ordered by the usual $\leq$ is a binomial poset with factrorial function $B(n) = 1$.
The poset of finite subsets of $\mathbb{P}$ ordered by inclusion is a binomial poset with factorial function $B(n) = n!$.
The poset of finite dimensional subspaces of an infinite dimensional vector space over $\mathbb{F}_q$ is a binomial poset with factorial function $B(n) = [n]_q!$.

Recall that an idempotent matrix A is such that $A^2 = A$. Let $\mathcal{E}_{n,q} = \mathcal{E}_n$ be the set of $n \times n$ idempotent matrices over $\mathbb{F}_q$. It is known (Cf. [9]) that $\mathcal{E}_n$ along with the relation $A \leq_1 B \Leftrightarrow AB = A$ and $BA = A$ is a poset. In fact, it is known that the set of idempotents of any semigroup along with $\leq_1$ is a poset (called the *natural partial order* Cf [10],[11]). The theorem below shows that on the set $\mathcal{E}_n$, $\leq_1$ is equivalent to the relation $A \leq_2 B \Leftrightarrow \text{null}A \supseteq \text{null}B$ and $\text{im}A \subseteq \text{im}B$.

Theorem 2.2. *The relation $\leq_1$ on the set $\mathcal{E}_n$ of $n \times n$ idempotent matrices over $\mathbb{F}_q$ defined by $A \leq_1 B \Leftrightarrow AB = A$ and $BA = A$ is equivalent to the relation $\leq_2$ on the same set defined by $A \leq_2 B \Leftrightarrow nullA \supseteq nullB$ and $imA \subseteq imB$.*

Proof. $\Rightarrow$ Let $A, B \in \mathcal{E}_n$. Assume $AB = A$ and $BA = A$. Let $\vec{v} \in \text{null}B$. Then $B\vec{v} = 0 \Rightarrow AB\vec{v} = 0 \Rightarrow A\vec{v} = 0 \Rightarrow \vec{v} \in \text{null}A$. Let $\vec{v} \in \text{im}A$. Then there is a $\vec{w}$ such that $A\vec{w} = \vec{v} \Rightarrow BA\vec{w} = \vec{v} \Rightarrow \vec{v} \in \text{im}B$.

$\Leftarrow$ Let $\vec{x} \in \mathbb{F}_q^n$. Assume $\text{null}A \supseteq \text{null}B$ and $\text{im}A \subseteq \text{im}B$. Then $\vec{x} = \vec{u_1} + \vec{v_1}$ where $\vec{u_1} \in \text{null}A, \vec{v_1} \in \text{im}A \subseteq \text{im}B$. So $A\vec{x} = A\vec{u_1} + A\vec{v_1} = 0 + A\vec{v_1} = \vec{v_1}$ where the last equality follows because $\vec{v_1} \in \text{im}A$. Also $B\vec{v_1} = \vec{v_1}$ so that $BA\vec{x} = A\vec{x}$.

We also have that $\vec{x} = \vec{u_2} + \vec{v_2}$ where $\vec{u_2} \in \text{null}B \subseteq \text{null}A, \vec{v_2} \in \text{im}B$. So $A\vec{x} = A\vec{u_2} + A\vec{v_2} = 0 + A\vec{v_2} = A\vec{v_2}$. Also, $B\vec{x} = B\vec{u_2} + B\vec{v_2} = 0 + \vec{v_2} = \vec{v_2}$ so that $AB\vec{x} = A\vec{x}$.

□

We note that the rank of a matrix A in $\mathcal{E}_n$ is simply its matrix rank. Also, $\hat{0}, \hat{1}$ are the zero matrix and the identitiy matrix respectively and the length of every maximal chain is n. The next theorem shows that if A is covered by B then there is a unique subspace U (necessarily of dimension 1) contained in null$A$ such that im$B$ = im$A \oplus U$.

Theorem 2.3. *Let $A, B \in \mathcal{E}_n$ with A covered by B. Then there is a unique subspace U of null$A$ such that im$B$ = im$A \oplus U$.*

Proof. (Existence) Let $\vec{v_1}, \ldots, \vec{v_r}$ be a basis for im$A$. Since im$A \subset$ im$B$ and dim(im$B$) = dim(im$A$) + 1, we may extend this basis to $\vec{v_1}, \ldots, \vec{v_r}, \vec{w}$, a basis for im$B$ for some $\vec{w} \in \mathbb{F}_q^n$. Now, A is idempotent so that $\mathbb{F}_q^n$ = im$A \oplus$ null$A$. So $\vec{w} = \vec{x} + \vec{y}$ for some $\vec{x} \in$ im$A$ and $\vec{y} \in$ null$A$. Then $\vec{x}$ is a linear combination of $\vec{v_1}, \ldots, \vec{v_r}$ so that $\vec{v_1}, \ldots, \vec{v_r}, \vec{y}$ is a basis for im$B$. Setting $U = \text{span}(\vec{y}) \subseteq$ null$A$ shows existence.

(Uniqueness) Suppose im$B$ = im$A \oplus U_1$ and im$B$ = im$A \oplus U_2$ for $U_1 = \text{span}(\vec{y_1}), U_2 = \text{span}(\vec{y_2}) \subseteq$ null$A$. Let $\vec{z} \in$ im$B -$ im$A$. Then $\vec{z} = a_1\vec{v_1} + \cdots a_r\vec{v_r} + a_{r+1}\vec{y_1} = b_1\vec{v_1} + \cdots b_r\vec{v_r} + b_{r+1}\vec{y_2}$ for some scalars a_i, b_i with $a_{r+1}, b_{r+1} \neq 0$. Subtracting the two expressions for $\vec{z}$ we have $\vec{0} = (a_1 - b_1)\vec{v_1} + \cdots (a_r - b_r)\vec{v_r} + a_{r+1}\vec{y_1} - b_{r+1}\vec{y_2}$. So that $(a_1 - b_1)\vec{v_1} + \cdots (a_r - b_r)\vec{v_r} = -a_{r+1}\vec{y_1} + b_{r+1}\vec{y_2}$. The LHS is in im$A$ so that $-a_{r+1}\vec{y_1} + b_{r+1}\vec{y_2} \in$ im$A$. But $\vec{y_1}, \vec{y_2} \in$ null$A$ so that $-a_{r+1}\vec{y_1} + b_{r+1}\vec{y_2} \in$ im$A \cap$ null$A = \vec{0}$. Then $a_{r+1}\vec{y_1} = b_{r+1}\vec{y_2}$. Multiplying by the inverse of a_{r+1} shows that $\vec{y_1}$ is a scalar multiple of $\vec{y_2}$ so that $U_1 = U_2$.

□

Let $\hat{0} = E_0, E_1, \ldots, E_n = \hat{1}$ be a maximal chain in $\mathcal{E}_n$. From the above theorems, each step E_{i-1}, E_i in the chain corresponds to a unique 1-dimensional subspace $U_i =$ null$E_{i-1} \cap$ im$E_i =$ span$(\vec{u_i})$ for some nonzero $\vec{u_i} \in \mathbb{F}_q^n$. Then each maximal chain corresponds to a list of n linearly independent vectors. So up to multiplication by a nonzero scalar in $\mathbb{F}_q$, each maximal chain corresponds to a basis for $\mathbb{F}_q^n$. So the number of maximal chains in $\mathcal{E}_n$ is $\frac{\gamma_n}{(q-1)^n}$. Then the factorial function for the binomial poset $\mathcal{E}$ is $B(n) = \frac{\gamma_n}{(q-1)^n}$

If we ignore the addition in the ring $\text{Mat}_n(\mathbb{F}_q)$ we have a semigroup where the operation is normal matrix multiplication. Each maximal subgroup in a semigroup contains (as its identity) exactly one idempotent element. Let $\mathcal{G}_E$ be the maximal subgroup of $\text{Mat}_n(\mathbb{F}_q)$ containing the idempotent E. Then $\mathcal{G}_E$ is isomorphic to $GL_r(\mathbb{F}_q)$ where r is the rank of E (Cf. 12).

Definition 2.4. Let $\vec{v} \neq \vec{0} \in \mathbb{F}_q^n$. Then $\vec{v}$ is a *reduced vector* if the first nonzero entry in $\vec{v}$ is 1. A basis for $\mathbb{F}_q^n$ whose vectors are all reduced vectors is called a *reduced basis.*

Let E_r be an idempotent at rank r in $\mathcal{E}_n$. Each saturated chain from $\hat{0}$ to E_r corresponds to a unique list of linearly independent vectors $\vec{u_1}, \ldots, \vec{u_r}$ where the vectors $\vec{u_i}$ are the reduced vectors such that $U_i = \text{span}(\vec{u_i})$. Let $\vec{b}_1, \ldots, \vec{b}_r$ be a basis for $\text{im}E_r$ where the $\vec{b}_i$ are the first r linearly independent columns of the matrix E_r. Then for each $i = \{1, \ldots, n\}$, the i^{th} column of E_r is a linear combination $a_{i,1}\vec{b}_1 + \cdots + a_{i,r}\vec{b}_r$ for some set $\{a_{i,1}, \ldots, a_{i,r}\}$ of scalars in $\mathbb{F}_q$. Let G_1 be the matrix whose i^{th} column is $a_{i,1}\vec{u}_1 + \cdots + a_{i,r}\vec{u}_r$. In other words, form the columns of G_1 with the same scalars in the linear combinations that determine the columns of E_r but substitute the vectors $\vec{u}_i$ in place of the vectors $\vec{b}_i$. Note that $\text{im}G_1 = \text{im}E_r$ because $\text{span}(\vec{b}_1, \ldots, \vec{b}_r) = \text{span}(\vec{u}_1, \ldots, \vec{u}_r)$. Also, $\text{null}G_1 = \text{null}E_r$ because the columns of each matrix have the same linear dependence relations. Form $G_2, G_3, \ldots, G_{(q-1)^r}$ similarly by replacing the reduced vectors $\vec{u}_i$ with all possible r-tuples of nonzero scalar multiples of the $\vec{u}_i$. Then $G_1, \ldots, G_{(q-1)^r} \in \mathcal{G}_{E_r}$.

Theorem 2.5. *The above construction performed over all saturated chains in $\mathcal{E}_n$ from $\hat{0}$ to E_r produces precisely the elements in $\mathcal{G}_{E_r}$, the maximal subgroup of $Mat_n(\mathbb{F}_q)$ containing E_r.*

Proof. First note that there are $\frac{\gamma_r}{(q-1)^r}$ saturated chains in $\mathcal{E}_n$ from $\hat{0}$ to E_r so that our construction over all such chains realizes exactly γ_r distinct matrices. By our comments above, each G_i has the same image and the same null space as E_r. This means that the set of all such G_i is precisely Green's $\mathcal{H}$-class containing E_r.

□

The reduced incidence algebra

The following definition is given in [8].

Definition 2.6. Let P be a locally finite poset, and let $\text{Int}(P)$ denote the set of intervals in P. Let K be a field. The *incidence algebra* $I(P, K) = I(P)$ is the K-algebra of all functions $f : \text{Int}(P) \to K$, along with the usual structure of a vector space over K and multiplication defined by

$$fg(s, u) = \sum_{s \leq t \leq u} f(s, t)g(t, u)$$

Let P be a binomial poset with factorial function $B(n)$. Then we may define the *reduced incidence algebra*

$$R(P) = \{f \in I(P) : \text{ if } l(s,t) = l(s',t') \text{ then } f(s,t) = f(s',t')\}.$$

where $l(s,t)$ denotes the length of the interval $[s,t]$.

Perhaps the most powerful motivation for our interest in binomial posets is that the reduced incidence algebra is isomorphic to the ring of formal power series. The isomorphism $\phi : R(P) \to \mathbb{C}[[u]]$ is given by

$$\phi(f) = \sum_{n \geq 0} f(n) \frac{u^n}{B(n)}.$$

where $f(n) = f(s,t)$ with $l(s,t) = n$.

Let $\delta \in R(P)$ be defined by

$$\delta(s,t) = \begin{cases} 1 & \text{if } s = t \\ 0 & \text{else} \end{cases}$$

Then δ is the identity function and the isomorphim maps δ to the formal power series 1.

Let $\eta \in R(P)$ be the incidence function that equals 1 if and only if s is covered by t. Then η is mapped to the formal power series u.

Perhaps the most useful function in the reduced incidence algebra is the zeta function ζ which simply assigns the value 1 to every interval in the poset. We will denote the image of the zeta function under the isomorphism as $E_P(u)$

$$\phi(\zeta) = \sum_{n \geq 0} \frac{u^n}{B(n)} := E_P(u)$$

In particular, for the binomial poset $\mathcal{E}_q = \mathcal{E}$ of all idempotent matrices over $\mathbb{F}_q$

$$\sum_{n \geq 0} \frac{u^n}{\frac{\gamma_n}{(q-1)^n}} := E_{\mathcal{E}}(u)$$

Since the zeta function assigns the value 1 to every interval, $\zeta^k(s,t)$ is equal to the number of length k multichains originating at s and ending at t. Also, $(\zeta - \delta)^k(s,t)$ is equal to the number of length k chains originating at s and ending at t. The elements A in the poset $\mathcal{E}$ can alternately be viewed as direct sum decompositions of $\mathbb{F}_q^n$ into $\text{im}A \oplus \text{null}A$. From these simple observations along with the isomorphism into formal power series we have the generating functions for the following counting sequences.

Let a_n be the number of reduced bases for $\mathbb{F}_q^n$.

$$\sum_{n\geq 0} a_n \frac{u^n}{\frac{\gamma_n}{(q-1)^n}} = \frac{1}{1-u}$$

Let a_n be the number of distinct subsets of vectors that are bases for $\mathbb{F}_q^n$. Equivalently a_n is the number of direct sum decompositions of $\mathbb{F}_q^n$ into 1-dimensional subspaces.

$$\sum_{n\geq 0} a_n \frac{u^n}{\frac{\gamma_n}{(q-1)^n}} = \exp(u)$$

Let a_n be the number of idempotent matrices in $\mathrm{Mat}_n(\mathbb{F}_q)$.

$$\sum_{n\geq 0} a_n \frac{u^n}{\frac{\gamma_n}{(q-1)^n}} = E_{\mathcal{E}}^2(u)$$

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

$$\sum_{n\geq 0}\sum_{k=0}^{n} a_{n,k} v^k \frac{u^n}{\frac{\gamma_n}{(q-1)^n}} = E_{\mathcal{E}}(vu)E_{\mathcal{E}}(u)$$

Let a_n be the number of relations in the poset $\mathcal{E}_n$, i.e., the number of ordered pairs (A, B) such that $A \leq B$ with $A, B \in \mathcal{E}_n$.

$$\sum_{n\geq 0} a_n \frac{u^n}{\frac{\gamma_n}{(q-1)^n}} = E_{\mathcal{E}}^3(u)$$

Let a_n be the number of covering relations in the poset $\mathcal{E}_n$, i.e., the number of ordered pairs (A, B) such that A is covered by B with $A, B \in \mathcal{E}_n$.

$$\sum_{n\geq 0} a_n \frac{u^n}{\frac{\gamma_n}{(q-1)^n}} = uE_{\mathcal{E}}^2(u)$$

Let a_n be the number of diagonalizable matrices in $\mathrm{Mat}_n(\mathbb{F}_q)$.

$$\sum_{n\geq 0} a_n \frac{u^n}{\frac{\gamma_n}{(q-1)^n}} = E_{\mathcal{E}}^q(u)$$

Let a_n be the number of diagonalizable matrices in $\mathrm{Mat}_n(\mathbb{F}_q)$ having rank k.

$$\sum_{n\geq 0}\sum_{k=0}^{n} a_{n,k} v^k \frac{u^n}{\frac{\gamma_n}{(q-1)^n}} = E_{\mathcal{E}}(u)E_{\mathcal{E}}^{q-1}(vu)$$

Let $a_{n,k}$ be the number of diagonalizable matrices in $GL_n(\mathbb{F}_q)$ with exactly k distinct eigenvalues.

$$\sum_{n\geq 0}\sum_{k=0}^{q} a_{n,k}v^k\frac{u^n}{\frac{\gamma_n}{(q-1)^n}} = (vE_{\mathcal{E}}(u) - v + 1)^q$$

Let a_n be the number of direct sum decompositions of $\mathbb{F}_q^n$.

$$\sum_{n\geq 0} a_n\frac{u^n}{\frac{\gamma_n}{(q-1)^n}} = \exp(E_{\mathcal{E}}(u) - 1)$$

Let $a_{n,k}$ be the number of direct sum decompositions of $\mathbb{F}_q^n$ into exactly k subspaces.

$$\sum_{n\geq 0}\sum_{k=0}^{q} a_{n,k}v^k\frac{u^n}{\frac{\gamma_n}{(q-1)^n}} = \exp(v(E_{\mathcal{E}}(u) - 1))$$

Let a_n be the number of *periodic* matrices, i.e., elments that are contained in some (maximal) subroup of $\mathrm{Mat}_n(\mathbb{F}_q)$. In other words, $a_n = \sum_{e\in\mathcal{E}_n} |G_e|$.

$$\sum_{n\geq 0} a_n\frac{u^n}{\frac{\gamma_n}{(q-1)^n}} = E_{\mathcal{E}}(u)/(1 - (q-1)u)$$

Let $a_{n,k}$ be the number of ordered direct sum decompositions of $\mathbb{F}_q^n$ into exactly k subspaces.

$$\sum_{n\geq 0}\sum_{k=0}^{q} a_{n,k}v^k\frac{u^n}{\frac{\gamma_n}{(q-1)^n}} = 1/(1 - v(E_{\mathcal{E}}(u) - 1))$$

Substituting $v = -1$ in the generating function above gives $\frac{1}{E_{\mathcal{E}}(u)}$ (the image of the Moebius function μ under our isomorphism). So for the poset $\mathcal{E}_n$, we have that $\mu(\hat{0}, \hat{1})$ is equal to the number of ordered direct sum decompositions of $\mathbb{F}_q^n$ into an even number of subspaces minus the number of such decompositions into an odd number of subspaces. This is an instance of Phillip Hall's Theorem.

$\mathcal{E}_n$ as a Segre product of binomial posets

In this subsection we follow the ideas in [8, Section 3.18] to describe $\mathcal{E}_n$ as a Segre product of two binomial posets as suggested in [16]. The following definition is given in [8].

Definition 2.7. Let $P_1, \ldots, P_k$ be binomial posets with factorial functions $B_1(n), \ldots, B_k(n)$. Let P be the subposet of $P_1 \times \cdots \times P_k$ consisting of all k-tuples $(t_1, \ldots t_k)$ such that $\text{rank}(t_1) = \cdots = \text{rank}(t_k)$. Then P is a binomial poset with factorial function $B_1(n) \cdots B_k(n)$. We write $P = P_1 * \cdots * P_k$, the *Segre product* of $P_1, \ldots, P_k$.

Let P be the poset of all finite dimensional subspaces of a vector space of infinite dimension over $\mathbb{F}_q$ ordered by inclusion ($A \leq B$ iff $A \subseteq B$). Then P is a binomial poset with factorial function $B(n) = [n]_q! = \frac{\gamma_n}{(q-1)^n q^{\binom{n}{2}}}$. Let P_n denote the familiar lattice of subspaces of $\mathbb{F}_q^n$ ordered by inclusion. Then P_n is isomorphic to an n-interval in P.

Let Q be the set of all complementary subspaces of the standard complete flag, $\{\vec{0}\} \subseteq \langle e_1 \rangle \subseteq \langle e_1, e_2 \rangle \subseteq \langle e_1, e_2, e_3 \rangle \cdots$. Then Q along with subspace containment ($A \leq B$ iff $A \supseteq B$) is a binomial poset with factorial function $q^{\binom{n}{2}}$. Indeed, fix n, k. There are $q^{k(n-k)}$ complementary subspaces of $\langle e_1, e_2, \ldots, e_k \rangle$ Cf.[18]. In particular, there are q^{n-1} atoms in any n-interval of Q. Then $B(n) = A(n)A(n-1) \cdots A(1) = q^{n-1}q^{n-2} \cdots q = q^{\binom{n}{2}}$ where $A(m)$ denotes the number of atoms in an m-interval.

Let Q_n denote the lattice of subspaces that are complementary to $\mathcal{F}_0$ the standard flag $\{\vec{0}\} \subseteq \langle e_1 \rangle \subseteq \langle e_1, e_2 \rangle \subseteq \cdots \subseteq \langle e_1, e_2, \ldots e_n \rangle$ in $\mathbb{F}_q^n$. Then Q_n is isomorphic to any n-interval in Q.

Definition 2.8. Let $\mathcal{B} = \langle \vec{v_1}, \ldots, \vec{v_n} \rangle$ be a basis for $\mathbb{F}_q^n$. Let $\mathcal{F}$ be a complete flag $\{\vec{0}\} = V_0 \subseteq V_1 \subseteq \cdots \subseteq V_n = \mathbb{F}_q^n$. Then $\mathcal{B}$ is *adapted* to the flag $\mathcal{F}$ if $V_i \subseteq \text{span}(v_1, \ldots, v_i)$ for all $i = 1, \ldots, n$.

We note that there are $(q-1)(q^2-q)(q^3-q^2)\cdots(q^n-q^{n-1}) = q^{\binom{n}{2}}(q-1)^n$ bases adapted to any given flag in $\mathbb{F}_q^n$. Let $GL_n(\mathbb{F}_q)$ act on the set of all complete flags in $\mathbb{F}_q^n$. The stabilizer subgroup of the standard flag is the set of upper triangular matrices. The stabilizer subgroup of an arbitrary complete flag $\mathcal{F}$ is the group of invertible upper triangular matrices with respect to any basis adapted to $\mathcal{F}$. In other words, if we let $GL_n(\mathbb{F}_q)$ act on the set of upper triangular matrices by conjugation then each row in the action table is the stabilizer subgroup of some complete flag. The number of complete flags in $\mathbb{F}_q^n$ is $\frac{\gamma_n}{q^{\binom{n}{2}}(q-1)^n} = [n]_q!$.

Theorem 2.9. *The poset $P_n * Q_n$ is isomorphic to the set $\{(U, W) : U \in P_n, W \in Q_n, \text{rank}(U) = \text{rank}(W)\}$ along with the relation: $(U_1, W_1) \leq (U_2, W_2)$ if and only if*

(i) there is a flag $\mathcal{F}_1$ in P_n that contains both U_1 and U_2.

(ii) there is a bijective linear map ϕ from the standard flag $\mathcal{F}_0$ to $\mathcal{F}_1$ such that $\phi(W_1) \supseteq \phi(W_2)$.

Proof. $\Leftarrow$ Assume $(U_1, W_1) \leq (U_2, W_2)$. By condition (i) $U_1 \leq_{P_n} U_2$. Let ϕ be a bijective linear map from the standard flag $\mathcal{F}_0$ to $\mathcal{F}_1$ such that $\phi(W_1) \supseteq \phi(W_2)$. Let Q_1 be the poset of complementary subspaces of $\mathcal{F}_1$ along with containment. Then ϕ is a poset isomorphism from Q_n to Q_1. Then $W_1 \supseteq W_2$ so that $W_1 \leq_{Q_n} W_2$.

$\Rightarrow$ Assume $U_1 \leq_{P_n} U_2$ and $W_1 \leq_{Q_n} W_2$. Then there is a flag $\mathcal{F}_1$ in P_n that contains both U_1 and U_2. Let ϕ be an $n \times n$ matrix whose columns are a basis adapted to $\mathcal{F}_1$. Then ϕ is a bijective linear map from the standard flag $\mathcal{F}_0$ to $\mathcal{F}_1$ such that $\phi(W_1) \supseteq \phi(W_2)$.

□

3. The cycle index for matrices

In this section we follow [4] in using the cycle index for matrices developed in [13] to derive bivariate generating functions that give enumerative results on various classes of matrices over a finite field. In like manner, we count the number of elements of any given order in $GL_n(\mathbb{F}_q)$. Our presentation provides a concise and uniform mechanism for solving matrix enumeration problems involving parameterizations of various properties of matrices.

The cycle index for matrices first developed by Kung [13] and then modified by Stong [14] is a vector space analog of the Polya cycle index for a permutation group. A beautiful exposition of which is given by Morrison in [4] and Fulman [15]. In its most rudimentary form the cycle index for matrices can be expressed as

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

where Φ is the set of all monic irreducible polynomials in $\mathbb{F}_q[x]$ and the indeterminants are subscripted by ϕ paired with the integer partition $\lambda_\phi(A)$ associated to ϕ by an $n \times n$ matrix A over a finite field $\mathbb{F}_q$. Many important enumeration results (Cf.[4]) can be realized by simply setting the indeterminants equal to 0 or 1 in accordance with the dictates of some desired class of matrices. Extending 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 involving parameterizations of various properties. 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 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 in the characteristic polynomial.

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

Periodic $n \times n$ matrices over $\mathbb{F}_q$ classified by nullity Cf. A348015

Order of invertible matrices Cf A346743.

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: $\phi^{\lambda_1} | \phi^{\lambda_2} | \cdots | \phi^{\lambda_j}$ (which in this case is also the set of elementary divisors). 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 [13]

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

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 $(\phi \in \Phi, \lambda \neq \emptyset \in L)$ determined by such a function is called the conjugacy class data in [4].

Fix $l \subseteq L, d \geq 1$. Let $\mathrm{length}(\lambda)$ denote the number of its parts and $\max(\lambda)$ be the largest part where it is understood that $\mathrm{length}(\emptyset) = 0$ 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 $\mathbf{Mat}_n(\mathbb{F}_q)$

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 nullity k, $0 \leq k \leq n$. Note that the variable v in $G_{1,l}$ is counting 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 whose primary rational canonical form has k blocks, i.e., T has k elementary divisors $0 \leq k \leq n$.

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

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. Note that $a_{n,1} = 2$ for $n \geq 1$ and that $a_{n,n}$ is the number of cyclic matrices. 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 $\{1 \leq 1 \leq \cdots \leq 1\}$. 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

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

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

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

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

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

Triangularizable matrices

A matrix T in $\mathrm{Mat}_n(\mathbb{F}_q)$ is *triangularizable* 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 $1 \leq i \leq n$. It is shown in [19] 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

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

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 nullity 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 nullity $k,\ 0 \leq k \leq n$. 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 the prime factorization of the minimal polynomial. 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

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 isomorphic 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.

Periodic matrices

A matrix $T\in\mathrm{Mat}_n(\mathbb{F}_q)$ is *periodic* if $T=T^k$ for some $k>1$. Then T is periodic 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 $a_{n,k}$ be the number of periodic matrices in $\mathrm{Mat}_n(\mathbb{F}_q)$ with nullity k. Then

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

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

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

4. Torsion classes in $\mathrm{Mat}_n(\mathbb{F}_q)$

In this section we define an equivalence relation $\sim_D$ on $\mathrm{Mat}_n(\mathbb{F}_q)$. We define two refinements of $\sim_D$, and count the number of classes in each relation and the number of matrices in each class. We also give an expression for the $n \to \infty$ limiting probability that a random $n \times n$ matrix is periodic.

Let $A \in \mathrm{Mat}_n(\mathbb{F}_q)$. Then for some $k,\ 1 \leq k < n$

$$\mathrm{im}(A) \supseteq \mathrm{im}(A^2) \supseteq \cdots \supseteq \mathrm{im}(A^k) = \mathrm{im}(A^{k+1}) = \mathrm{im}(A^{k+2}) \cdots$$

So for a sufficiently large (say n) power of A the subsequent images in the above sequence are stable, i.e., they are all the same subspace.

Let $\sim_D$ be the equivalence relation on $\mathrm{Mat}_n(\mathbb{F}_q)$ defined by

$$A \sim_D B \text{ if and only if } \mathrm{rank}(A^n) = \mathrm{rank}(B^n) \text{ for all } A, B \in \mathrm{Mat}_n(\mathbb{F}_q)$$

In other words, $A \sim_D B$ if and only if A^n and B^n are in the same $\mathcal{D}$-class of Green's $\mathcal{D}$ relation on $\mathrm{Mat}_n(\mathbb{F}_q)$. Since the dimension of any $n \times n$ matrix is in $\{0, 1, 2, \ldots, n\}$, the number of equivalence classes under $\sim_D$ is $n + 1$. In order to count the size of each class we investigate two important classes of matrices: periodic matrices and nilpotent matrices.

A matrix $T \in \mathrm{Mat}_n(\mathbb{F}_q)$ is periodic if $T = T^j$ for some $j > 1$. The following are equivalent Cf. [12].

(i) T is periodic

(ii) $\mathrm{im}(T) = \mathrm{im}(T^2)$

(iii) $\mathrm{rank}(T) = \mathrm{rank}(T^2)$

(iv) z^2 does not divide $m_T(z)$, the minimal polynomial of T.

(v) $\mathbb{F}_q^n = \mathrm{im}(T) \oplus \mathrm{null}(T)$.

(vi) T is in a subgroup of $\mathrm{Mat}_n(\mathbb{F}_q)$

(vii) T is similar to a block diagonal matrix of the form $\begin{pmatrix} P & 0 \\ 0 & 0 \end{pmatrix}$ for some invertible matrix P.

Let R_n be the number of periodic matrices in $\mathrm{Mat}_n(\mathbb{F}_q)$. Let $G(u, \mathbf{x})$ be the generating function for the cycle index for matrices. Cf. [1],[2].

$$\begin{aligned} G(u,\mathbf{x}) &:= \sum_{n\geq 0} \frac{u^n}{\gamma_n} \sum_{A\in \mathrm{Mat}_n(\mathbb{F}_q)} \prod_{\phi\in\Phi} x_{\phi,\lambda_\phi(A)} \\ &= \prod_{\phi\in\Phi} \sum_{\lambda\in L} \frac{x_{\phi,\lambda} u^{|\lambda|\deg\phi}}{c_\phi(\lambda)} \\ &= (\sum_{\lambda\in L} \frac{x_{z,\lambda}u^{|\lambda|}}{c_z(\lambda)})(\prod_{\phi\in\Phi-\{z\}} \sum_{\lambda\in L} \frac{x_{\phi,\lambda}u^{|\lambda|\deg\phi}}{c_\phi(\lambda)}) \end{aligned}$$

Set $x_{z,\lambda} = 1$ if $\lambda \in \{\emptyset, \{1\}, \{1,1\}, \{1,1,1\}\cdots\}$ and 0 otherwise. Set $x_{\phi,\lambda} = 1$ for all $\phi \in \Phi - \{z\}$. Now $c_z(\{1^n\}) = \gamma_n$. So we have:

$$\sum_{n\geq 0} \frac{R_n u^n}{\gamma_n} = (\sum_{n\geq 0} \frac{u^n}{\gamma_n})(\prod_{\phi\in\Phi-\{z\}} \sum_{\lambda\in L} \frac{u^{|\lambda|\deg\phi}}{c_\phi(\lambda)})$$

The product on the right hand side counts the invertible matrices so that

$$\sum_{n\geq 0} \frac{R_n u^n}{\gamma_n} = (\sum_{n\geq 0} \frac{u^n}{\gamma_n})(\frac{1}{1-u}) \qquad (1)$$

Extracting the coefficients gives

$$R_n = \sum_{d=0}^{n} \frac{\gamma_n}{\gamma_{n-d}}$$

Probability that a random matrix is periodic

Let $P(R_n)$ be the $n \to \infty$ limiting probability that a random $n \times n$ matrix is recurrent. From [5] we have:

Lemma [15] If $f(u)$ has a Taylor series about 0 and $f(1) < \infty$ then

$$\lim_{n\to\infty}[u^n]\frac{1}{1-u}f(u) = f(1)$$

Proof: Write $f(u)$ as its Taylor series about 0 and view $\frac{1}{1-u}f(u)$ as the product of two ordinary generating functions. Then we see the coefficients in the expansion are the partial sums of the coefficients in the expansion of $f(u)$.

$$\frac{1}{1-u}f(u) =$$

$$\frac{1}{1-u}(f(0) + f'(0)u + \frac{f''(0)u^2}{2!} + \frac{f'''(0)u^3}{3!} + \cdots) =$$

$$f(0) + (f(0) + f'(0))u + (f(0) + f'(0) + \frac{f''(0)}{2!})u^2 + \cdots + \sum_{i=0}^{n}\frac{f^i(0)}{i!}u^n + \cdots$$

So that

$$\lim_{n\to\infty}[u^n]\frac{1}{1-u}f(u) = \lim_{n\to\infty}\sum_{i=0}^{n}\frac{f^i(0)}{i!} = f(1) \quad \square.$$

It follows from the above lemma and (1) that:

$$\lim_{n\to\infty} P(R_n) = (\prod_{i\geq 1} 1 - \frac{1}{q})(\sum_{n\geq 0}\frac{1}{\gamma_n})$$

Let $R_{n,d}$ be the number of periodic matrices in $\mathrm{Mat}_n(\mathbb{F}_q)$ having rank d.

$$\sum_{n\geq 0}\sum_{d=0}^{n}\frac{R_{n,d}v^d u^n}{\gamma_n} = (\prod_{\phi\in\Phi-\{z\}}\sum_{\lambda\in L}\frac{(vu)^{|\lambda|\deg\phi}}{c_\phi(\lambda)})(\sum_{n\geq 0}\frac{u^n}{\gamma_n})$$

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

So that

$$R_{n,d} = \frac{\gamma_n}{\gamma_{n-d}}$$

We note that the values $R_{n,d}$ can also be generated by the recurrence

$$R_{n,d} = R_{n,d-1} \cdot R_{n-d+1,1}$$

with $R_{n,0} = R_{1,1} = 1$.

Let N_n be the number of $n \times n$ nilpotent matrices. It has been shown in many ways that for $n \geq 1,\ N_n = q^{n(n-1)}$. We derive the generating function using the factorization given in [Morrison]: Fix $\phi \in \Phi$, then

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

So we have

$$G(u, \mathbf{x}) = \prod_{\phi \in \Phi} \sum_{\lambda \in L} \frac{x_{\phi,\lambda} u^{|\lambda| \deg \phi}}{c_\phi(\lambda)}$$

Set $x_{\phi,\lambda} = 0$ for all $\phi \in \Phi - \{z\}$ and $x_{z,\lambda} = 1$. Then

$$1 + \sum_{n \geq 1} \frac{N_n u^n}{\gamma_n} = \sum_{\lambda \in L} \frac{u^{|\lambda|}}{c_z(\lambda)} = \prod_{r \geq 1} \frac{1}{1 - \frac{u}{q^r}}$$

Let $N_{n,k}$ be the number of $n \times n$ Nilpotent matrices with index $k,\ 1 \leq k \leq n$

$$1 + \sum_{n \geq 1} \sum_{k=0}^{n} \frac{N_{n,k} v^k u^n}{\gamma_n} = \sum_{\lambda \in L} \frac{v^{|\lambda_1|} u^{|\lambda|}}{c_z(\lambda)}$$

where λ_1 is the greatest part in λ.

Let A be a periodic matrix with $\text{rank}(A) = d,\ 0 \leq d \leq n$. Let $[A]_D = \{B \in \text{Mat}_n(\mathbb{F}_q) : A \sim_D B\}$. We decompose the matrices in $[A]_D$ into their invertible and idempotent parts. Observe that there are $R_{n,d} \cdot N_{n-d,1} = R_{n,d}$ matrices in $[A]_D$ whose idempotent part has index 1. There are $R_{n,d} \cdot N_{n-d,2}$ matrices in $[A]_D$ whose idempotent part has index 2 (these are the matrices in $[A]_D$ having rank $d+1$). Generally, for $k \geq 0$ the number of matrices in $[A]_D$ with rank $d+k$ is $R_{n,d} \cdot N_{n-d,k+1}$. Summing over k we have

$$|[A]_D| = \sum_{k \geq 0} R_{n,d} \cdot N_{n-d,k+1} = R_{n,d} \cdot N_{n-d} = \frac{\gamma_n}{\gamma_{n-d}} \cdot q^{(n-d)(n-d-1)}.$$

A refinement of $\sim_D$

Let $\sim_R$ be the equivalence relation on $\text{Mat}_n(\mathbb{F}_q)$ defined by

$$A \sim_R B \text{ if and only if } \text{im}(A^n) = \text{im}(B^n) \text{ for all } A, B \in \text{Mat}_n(\mathbb{F}_q)$$

In other words, $A \sim_R B$ if and only if A^n and B^n are in the same $\mathcal{R}$-class of Green's $\mathcal{R}$ relation on $\text{Mat}_n(\mathbb{F}_q)$. Then $\sim_R$ is a refinement of $\sim_D$. There are $\mathcal{G}_n$ classes in the relation.

Let A be a periodic matrix with $\text{rank}(A) = d,\ 0 \leq d \leq n$. Let $[A]_R = \{B \in \text{Mat}_n(\mathbb{F}_q) : A \sim_R B\}$.

The number of matrices in $[A]_R$ is equal to the number of matrices in $[A]_D$ divided by $\binom{n}{d}_q$ the number of d-dimensional subspaces of $\mathbb{F}_q^n$.

$$|[A]_R| = \frac{|[A]_D|}{\binom{n}{d}_q} = \frac{\gamma_n}{\gamma_{n-d}\binom{n}{d}_q} \cdot q^{(n-d)(n-d-1)}.$$

A refinement of $\sim_R$

Now we define the equivalence relation $\sim_K$ on $\text{Mat}_n(\mathbb{F}_q)$ by

$$A \sim_K B \text{ if and only if } A^j = B^k \text{ for some } j, k \geq 1$$

In other words, $A \sim_K B$ if and only if A and B are eventually (upon iteration) both equal to some idempotent $E \in \mathcal{E}_n$. If $A^j = B^k$ then $A^{jn} = B^{kn}$. So $\text{im}(A^n) = \text{im}(B^n)$. So that $\sim_K$ is a refinement of $\sim_R$.

Let $A \in \mathrm{Mat}_n(\mathbb{F}_q)$. Then there exist smallest positive integers k, m such that $\langle A \rangle = \{A, A^2, \ldots A^k, A^{k+1}, \ldots, A^{k+m-1}\}$ are distict elements and $A^k = A^{k+m}$. The set $\langle A \rangle$ being closed on multiplication forms a subsemigroup of $\mathrm{Mat}_n(\mathbb{F}_q)$ and is called the monogenic subsemigroup generated by A. The integer k is called the index of A and the integer m is called the period of A, while the order of A is $k + m - 1$. The elements $\{A^k, \ldots A^{k+m-1}\}$ form a cyclic subgroup where the identity is an idempotent $E = A^{k+i}$ where i is the smallest nonnegative integer such that $k + i$ is congruent to 0 modulo m.

From our work in sections 2 and 3, letting I_n denote the number of idempotent matrices in $\mathcal{E}_n$ we have

$$\sum_{n\geq 0} \frac{I_n u^n}{\gamma_n} = (\sum_{n\geq 0} \frac{u^n}{\gamma_n})^2$$

Extracting coefficients

$$I_n = \sum_{d=0}^{n} \frac{\gamma_n}{\gamma_d \cdot \gamma_{n-d}}$$

where the terms in the sum give $I_{n,d}$ the number of idempotent matrices having rank d.

Then the number of equivalence classes under the relation $\sim_K$ is I_n. For $E \in \mathcal{E}_n$ with $\mathrm{rank}(E) = d$

$$|[E]_K| = \frac{|[E]_R|}{\frac{I_{n,d}}{\binom{n}{d}_q}} = \gamma_d \cdot q^{(n-d)(n-d-1)}.$$

The equivalence classes $[E]_K$ are called the torsion classes of $\mathrm{Mat}_n(\mathbb{F}_q)$ corresponding to the idempotent E. Cf [17]

References

[1] Peter Doubilet, Gian-Carlo Rota and Richard Stanley, On the foundations of combinatorial theory VI: The idea of generating function, *Sixth Berkley Symposium on Mathematical Statistics and Probability Vol. II: Probability Theory*, University of California, (1972), 267-310.

[2] Richard Stanley, Binomial posets, Mobius inversion and permutation enumeration, *Journal of Combinatorial Theory* Vol. 20, (1976) 336-356.

[3] Phillipe Flajolet and Robert Sedgewick, Analytic Combinatorics, Cambridge University Press, 2009.

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

[5] David Dummit and Richard Foote, Abstract Algebra, Wiley, 2003.

[6] Sunil K Chebolu and Jan Minac, *Counnting irreducible polynomials over finite fields using inclusion exclusion principle* , arXiv: 1001.0409.

[7] Math Overflow, Generalized Euler phi function, https://mathoverflow.net/users/354626/fr%c3%a9d
paulin

[8] Richard Stanley, Enumerative Combinatorics Vol I, Second Edition, Cambridge, 2012.

[9] P. Semrl, Endomorphisms of the poset of idempotent matrices, *Journal of Algebra*, Vol 536, 2019

[10] Wikipedia, *Nabooripad order*.

[11] Encyclopedia of Mathematces, *Idempotent Matrix*

[12] Jan Okninski, *Semigroups of Matrices*, World Scientific Publishing Co., 1998.

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

[14] Richard Stong, Some assymptotic results on finite vector spaces, *Adv. in Appl. Math.* **9** (1988) 167-199.

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

[16] Math Overflow, *What alternatives are there to the binomial poset theory of generating function families?*, Keshav Srinivasan

[17] Encyclopedia of Mathematics, *Periodic semigroups.*

[18] David Ellerman, *The number of direct sum decompositions of a finite vector space*, ArXiv 1603.07619.

[19] Pete Clark, *Linear algebra: invariant subspaces* UGA Math.

[20] Richard Ehrenborg, Margarett Readdy *Classification of the factorial functions of Eulerian posets and Sheffer posets*, arXiv:math 0503303v2, (2006).

[21] Edward Bender, Jay Goldman, and G.C. Rota *Enumerative uses of generating functions*, Indiana University Mathematics Journal, Vol 20, No. 8, (1971), pp. 753-765.

Geoffrey Critzer 904 Central Ave. Dodge City KS 67801
Email address: gcritzer@ku.edu