Mark Hull
Portland State University

Susan Loepp
Bethel College

Matthew McGillis
Oregon State University

An Exploration into the Cycle Lengths of Matrices

Introduction: The things we show in this paper are:

I. Given an nxn matrix with entries that are elements of a field of characteristic p ($\mathbb{F}_p$), find all possible cycle lengths ω of the matrix.

II. Given an nxn matrix with entries that are elements of a field of characteristic p ($\mathbb{F}_p$), calculate the number of Jordan forms with cycle length ω.

III. Given an nxn matrix with entries that are elements of a field of characteristic p ($\mathbb{F}_p$), calculate the number of matrices with cycle length ω for non-derogatory case.

Part I

Consider a matrix A with coefficients in a field $\mathbb{F}_p$. We define the cycle length of A to be $\omega = |k-r|$ where k and r represent the first time that $A^k = A^r$. We will denote the characteristic polynomial of A by X_A. The characteristic polynomial can be factored into powers of irreducible polynomials:

$$X_A = p_1^{e_1} \cdot p_2^{e_2} \cdots p_s^{e_s}$$

Where P_i are all irreducible of degree d_i with coefficients in our field $\mathbb{F}_p$. We know that we can find a matrix J in Jordan form similar to A with coefficients in the algebraic closure of $\mathbb{F}_p$. Now, there exists an invertible matrix Q such that

$$QAQ^{-1} = J$$

So that,

$$A^n = Q^{-1} J^n Q$$

Hence if

$$A^k = A^r$$

then

$$Q^{-1} J^k Q = Q^{-1} J^r Q$$

or

$$J^k = J^r$$

So a matrix A has the same cycle length as its Jordan form.

Theorem: Suppose A has Jordan form J. Then there exists an h such that when $p^h \geq \upsilon$, where υ is the size of the biggest Jordan block, J^{p^h} is diagonal.

Proof: We can write every Jordan block, J, in this form $J = \lambda I + N$ where N is a nilpotent matrix such that $N^{\upsilon} = 0$.

Then,

$$J^{p^h} = \lambda^{p^h} I + \sum_{i=1}^{p^h} \binom{p^h}{i} \lambda^{p^h - i} N^i = \lambda^{p^h} I.$$

because $\binom{p^h}{i} - 0$ when $1 \leq i \leq p^h - 1$ and $N^{p^h} - 0$. [3]

Consider an irreducible polynomial P of degree d. We know that all of the roots of P will exist in $\mathbb{F}_{p^d}$. Now, if we exclude the zero element of this field, we are left with a multiplicative group $\mathbb{F}^{x}_{p^d}$ of order $P^d - 1$. By LaGrange's theorem, we know that the order of an element divides the order of the group where the order of an element λ is the smallest power μ such that $\lambda^{\mu} = 1$. Therefore, μ divides $p^{d}-1$. Now, let $e_0 =$ lcm [orders of roots of the characteristic polynomial (μ)], where lcm denotes least common multiple. Then $\lambda_i^{e_0} = 1$ if $\lambda_i \neq 0$. Let h_0 be the smallest integer such that $p^{h_0} \geq \upsilon$. Then we have the following theorem.

Theorem: $J^{e_0 p^{h_0}} = H$ where H is a diagonal matrix with ones and/or zeros on the diagonal. [3]

Notice that $p^{d}-1 = -1 \bmod p$, so p is not a divisor of $p^{d}-1$. Therefore, p does not divide μ for any λ. Hence, p^{h_0} and e_0 are relatively prime. Thus, the cycle lengths of an nxn matrix are of the form $e_0\, p^{h_0}$.

Part II

A. Given an irreducible polynomial q(x) and p find the cycle length k of the roots.

If $x^{k}-1-q(x)t(x) = 0$ and λ is a root of q(x)

$\lambda^{k}-1-q(\lambda)t(\lambda)=0$

$\lambda^{k}=1$

then $k =$ the smallest k such that q(x) divides $x^{k}-1$. [2]

B. Calculation of the number of irreducible polynomials of degree d with coefficients over $\mathbb{F}_p$ whose roots are ω-th roots of unity in $\mathbb{F}^{x}_{p^d}$.

We start with the following lemma.

Lemma: Let λ be an element of $\mathbb{F}^{x}_{p^d}$ and let ω divide p^d-1. Then λ^{ω} has minimal polynomial with coeficients of $\mathbb{F}_p$ of degree d if and only if $\frac{p^d-1}{\omega}$ does not divide p^g-1 for all $g < d$.

Now, we know that

$$\mathbb{F}^{x}_{p^d} \cong \mathbb{Z}/(p^d-1)\mathbb{Z} \quad ; \text{where } \cong \text{ denotes group isomorphism.}$$

We also know that

$$\mathbb{Z}/(p^d-1)\mathbb{Z} \cong \mathbb{Z}/q_1^{e1}\mathbb{Z} \times \mathbb{Z}/q_2^{e2}\mathbb{Z} \times \cdots \times \mathbb{Z}/q_t^{et}\mathbb{Z}$$

where

$$p^d-1 = q_1^{e1} q_2^{e2} \cdots q_t^{et} \qquad ; \text{ q's being prime.}$$

Consider ω such that ω divides p^d-1. Then ω can be factored as product of the following primes:

$$\omega = q_1^{f_1} q_2^{f_2} \cdots q_t^{f_t} \qquad ; \text{ q's being prime.}$$

We have the following :

The number of elements in $\mathbb{Z}/(p^d-1)\mathbb{Z}$ of order ω is equal to the product of the number elements in $\mathbb{Z}/q_i^{e_i}\mathbb{Z}$ of orders $q_i^{f_i}$. If we can find out how many elements of order p^r are in $\mathbb{Z}/p^s\mathbb{Z}$ for $r \geq s$ our problem is done. This is the same as counting the elements of $\{0,1,2,\ldots\ldots\ldots,p^s-1\}$ which are relatively prime to p^r. This is given by the Euler phi function

$$\phi(p^r) = p^r - p^{r-1} \qquad ; \text{p prime.}$$

So that the number of elements in $\mathbb{Z}/(p^d-1)\mathbb{Z} \cong \mathbb{F}^{x}_{p^d}$ which are ω-th roots of unity is

$$\phi(\omega) = \phi(q_1^{f_1})\phi(q_2^{f_2})\cdots\phi(q_t^{f_t}).$$

Since roots of polynomials or degree d come in sets of d conjugates, the number of irreducible polynomials in $\mathbb{F}_p[x]$ with roots in $\mathbb{F}^{x}_{p^d}$ that are ω-th roots of unity is given by:

$$\tau(d, \omega) - \phi(\omega) / d.$$

C. Given the cycle length,ω, of the roots and p find all irreducible polynomials.

We have already described a method to find the degree and the number of irreducible polynomials. Now, we can go through all possible polynomials of degree d and test all elements of $\mathbb{F}_p$ to see if they are roots of such a polynomial. When we find a polynomial with no roots in the base field, use part A to find the cycle length, α, of that polynomial. If $\alpha - \omega$, this is one of the irreducible polynomials we are looking for. We can go through this process until we have found all such polynomials (we know how many to look for from part B).

D. Given Jordan form, p and the size of the matrix, find the cycle length of the matrix.

We must find a k such that $p^k \geq \upsilon$. Then, we can use part A to get the order of each root of the irreducible polynomials of the characteristic polynomial. Then, by the theory described in part I, we can take $p^k e_0$ to get the cycle length of the matrix.

E. Given ω, n, and p, calculate the number of Jordan forms up to similarity.

Since p^{h_0} and e_0 are relatively prime, we can divide w by the greatest power of p that will divide it without remainder, k, and our result will be the least common multiple of the orders of roots of our characteristic polynomial. Then we know that $p^{k-1} < \upsilon \leq p^k$. From part B, we know the number of irreducible polynomials, $\tau(\omega, d)$, with cycle length ω and their degree d. Now we are left with a combinatorics problem of going through all possible combinations of d_i such that $n=\sum_{i=1}^{s} e_i d_i$ where, e_i is the multiplicity of the irreducible polynomial P_i of degree d_i.

Part III.

If we consider only invertible nxn matrices, then the following group theory applies. Let $GL_n(\mathbb{F}_p)$ represent the set of nxn invertible matrices with entries over the field $\mathbb{F}_p$; $GL_n(\mathbb{F}_p)$ is a group with the operation of matrix multiplication. For A, an element of $GL_n(\mathbb{F}_p)$, a conjugate of A, is any matrix of the form PAP^{-1} where P is also an element of $GL_n(\mathbb{F}_p)$. The relation "A is equal to a conjugate of B, or A is similar to B" is an equivalence relation in $GL_n(\mathbb{F}_p)$. Thus, the relation ~ partitions $GL_n(\mathbb{F}_p)$ into equivalency (or conjugacy) classes. For any A, an element of $GL_n(\mathbb{F}_p)$, the centralizer of A, written C_A, is the set of all the matrices in $GL_n(\mathbb{F}_p)$ which commute with A.

$$C_A = (X \text{ in } GL_n(\mathbb{F}_p) : XAX^{-1} = A)$$

C_A is a subgroup of $GL_n(\mathbb{F}_p)$ and thus its order divides the order of $GL_n(\mathbb{F}_p)$. We can say something further, that is,if we know the order of $GL_n(\mathbb{F}_p)$ and the order of the centralizer of A then the number of distinct conjugates of A is equal to the index of C_A in $GL_n(\mathbb{F}_p)$ written $(GL_n(\mathbb{F}_p) : C_A)$.

$$(GL_n(\mathbb{F}_p) : C_A) = | GL_n(\mathbb{F}_p) | / | C_A |$$

where the order of $GL_n(\mathbb{F}_p)$ is given by:

$$| GL_n(\mathbb{F}_p) | = \prod_{i=0}^{n-1} (p^n - p^i).$$

We can count the number of Jordan form matrices corresponding to a given cycle length. If we knew the order of the centralizer of a given Jordan form J then we could calculate the number of conjugugates of J. We showed in Part I that if A~J then A and J have the same cycle length. So, knowing the number of conjugates we could exactly determine the number of matrices in $GL_n(\mathbb{F}_p)$ with a given cycle length.

For a special case, we can calculate the order of the centralizer.

Definition: Let A be in $GL_n(\mathbb{F}_p)$. A is nonderogatory if the minimal and characteristic polynomials of A are equal.

In order to calculate the number of conjugates of A we have the following theorem:

Theorem: Let A be in $GL_n(\mathbb{F}_p)$ with the following minimal and characteristic polynomials

$$m_A(x) = X_A(x) = P_1^{e_1} \cdot P_2^{e_2} \cdots P_s^{e_s}$$

where P_i's are irreducible polynomials in x. Let degree of each $P_i = d_i$. Then the number of invertible matrices commuting with A is:

$$|C_A| = \prod_{j=1}^{s} \phi(p^{d_j})$$

where $\phi(u)$ is the Euler phi function. [1]

Therefore, the number of conjugates of A is:

$$|GL_n(\mathbb{F}_p)| / |C_A| = \prod_{i=0}^{n-1} (p^n - p^i) / \prod_{j=1}^{s} \phi(p^{d_j})$$

References

] Carlitz, L. and John H. Hodges: Distribution of Matrices in a Finite Field. Pacific Journal of Mathematics. 6, 225-230 (1956).

] Elspas, Bernard: The Theory of Autonomous Linear Sequential Networks. IRE Trans. CT-6, 45-60 (1959).

] Hellegouarch, Yves: Periodicite Des Puissances D'une Matrice dont les Coefficients Appartiennent a Un Corps Fini. Applications. C.R. Math. Rep. Acad. Sci. Canada. 8, 185-190 (1986).

Some Results

2 by 2 Matrix

Mod 2			Mod 3			Mod 5		
#of Times	Size of Loop	Reach Loop	#of Times	Size of Loop	Reach Loop	#of Times	Size of Loop	Reach Loop
8	1	0	14	1	0	32	1	0
3	1	1	8	1	1	24	1	1
3	2	0	25	2	0	61	2	0
2	3	0	8	3	0	20	3	0
			6	4	0	212	4	0
			8	6	0	24	5	0
			12	8	0	20	6	0
						40	8	0
						24	10	0
						40	12	0
						48	20	0
						80	24	0

3 by 3 Matrix

58	1	0	236	1	0
105	1	1	1040	1	1
42	1	2	624	1	2
105	2	0	1873	2	0
112	3	0	936	2	1
42	4	0	1664	3	0
48	7	0	2106	4	0
			3536	6	0
			4212	8	0
			1728	13	0
			1728	26	0

4 by 4 Matrix

802	1	0
4515	1	1
6300	1	2
2520	1	3
4515	2	0
5040	2	1
9072	3	0
3360	3	1
8820	4	0
1344	5	0
5040	6	0
11520	7	0
2688	15	0