On the Regular Semisimple Elements and Primary Classes of $GL(n, q)$

Jamshid Moori[a], Ayoub Basheer[a,b]

[a] School of Mathematical Sciences, University of KwaZulu Natal, P Bag X01, Scottsville 3209, Pietermaritzburg, South Africa.
[b] Department of Applied Mathematics, Faculty of Mathematical Sciences, University of Khartoum, P. O. Box 321, Khartoum, Sudan.

3 Aug 2009

Abstract

In this talk we count the numbers of regular semisimple elements and primary classes of $GL(n, q)$. The approach used here depends essentially on partitions of positive integers $\leq n$. We give the numbers of regular semisimple elements and primary classes of $GL(n, q)$ for $n \in \{1, 2, \cdots, 6\}$ and see that the number of regular semisimple elements is an integral polynomial in q, while the number of primary classes is a rational polynomial in q.

The Group $GL(n, q)$

- The *General Linear Group* $GL(V)$ is the automorphism group of a vector space V.
- If V is a finite $n-$dimensional space defined over a filed $\mathbb{F}$, then $GL(V)$ is identified with $GL(n, \mathbb{F})$.
- We restrict ourselves to the case $\mathbb{F} = \mathbb{F}_q$, the *Galois Field* of q elements, and we denote $GL(n, \mathbb{F}_q)$ by $GL(n, q)$.
- $|GL(n, q)| = \prod_{k=0}^{n-1} (q^n - q^k)$.

Conjugacy Classes of $GL(n, q)$

- Let $f(t) = \sum_{i=0}^{d} a_i t^i \in \mathbb{F}_q[t],\ a_d = 1$. The $d \times d$ *companion matrix* $U(f) = U_1(f)$ of $f(t)$ is

$$U_1(f) = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \cdots & \cdots & \cdots & \ddots & \vdots \\ \vdots & \vdots & \vdots & \ddots & 1 \\ -a_0 & -a_1 & -a_2 & \cdots & -a_{d-1} \end{pmatrix},$$

Conjugacy Classes of $GL(n, q)$

- For any $m \in \mathbb{N}$, let $U_m(f)$ be the $md \times md$ matrix of blocks

$$U_m(f) = \begin{pmatrix} U_1(f) & I_d & \underline{0} & \cdots & \underline{0} \\ \underline{0} & U_1(f) & I_d & \cdots & \underline{0} \\ \cdots & \cdots & \cdots & \ddots & \vdots \\ \vdots & \vdots & \vdots & \ddots & I_d \\ \underline{0} & \underline{0} & \underline{0} & \cdots & U_1(f) \end{pmatrix}.$$

- If $\lambda = (\lambda_1, \lambda_2, \cdots, \lambda_k) \vdash n$ is a partition of n, then $U_\lambda(f)$ is defined to be $U_\lambda(f) = \bigoplus_{i=0}^{k} U_{\lambda_i}(f)$.

Conjugacy Classes of $GL(n, q)$

Theorem 1 (The Jordan Canonical Form)

Let $A \in GL(n, q)$ with characteristic polynomial $f_A = f_1^{z_1} f_2^{z_2} \cdots f_k^{z_k}$, where f_i, $1 \leq i \leq k$ are distinct irreducible polynomials over $\mathbb{F}_q[t]$ and z_i is the multiplicity of f_i. Then A is conjugate to a matrix of the form

$$\bigoplus_{i=1}^{k} U_{\nu_i}(f_i), \text{ where } \nu_i \vdash z_i.$$

- Thus any conjugacy class of $GL(n, q)$ is parameterized by the data of sequences $(\{f_i\}, \{d_i\}, \{z_i\}, \{\nu_i\})$, where for $1 \leq i \leq k$,
$$\sum_{i=1}^{k} z_i d_i = n, \ \nu_i \vdash z_i, \ f_i \in \mathbb{F}_q[t] \text{ is irreducible with } \partial f_i = \deg(f_i) = d_i.$$

Conjugacy Classes of $GL(n, q)$

- The integer k is called the *length* of the data.
- Two data $(\{f_i\}, \{d_i\}, \{z_i\}, \{\nu_i\})$ and $(\{g_i\}, \{e_i\}, \{w_i\}, \{\mu_i\})$ with lengths k and $k^{'}$ respectively parameterize the same conjugacy class if $k = k^{'}$ and $\exists\ \sigma \in S_k$ such that

$$w_i = z_{\sigma(i)},\ e_i = d_{\sigma(i)},\ \mu_i = \nu_{\sigma(i)} \quad \text{and} \quad g_i = f_{\sigma(i)}, \quad \forall i.$$

- Two classes of $GL(n, q)$ parameterized by the above data are said to be of the same *type* if $k = k^{'}$ and $\exists\ \sigma \in S_k$ such that

$$w_i = z_{\sigma(i)},\ e_i = d_{\sigma(i)} \quad \text{and} \quad \mu_i = \nu_{\sigma(i)}$$

(g_i and f_i are allowed to differ).

Conjugacy Classes of $GL(n, q)$

Definition 2

Let c be a conjugacy class given by $(\{f_i\}, \{d_i\}, \{z_i\}, \{\nu_i\})$ with length k, then

1. c is called *primary class* if and only if $k = 1$.
2. c is called *regular class* if and only if $l(\nu_i) \leq 1, \ \forall \ 1 \leq i \leq k$.
3. c is called *semisimple class* if and only if $l(\nu_i{}') \leq 1, \ \forall \ 1 \leq i \leq k$.
4. c is called *regular semisimple class* if it is both regular and semisimple. Alternatively, a class is regular semisimple if and only if $\nu_i = 1, \ \forall \ 1 \leq i \leq k$.

Size of Conjugacy Classes of $GL(n, q)$

- Let $\phi_r(t) = \prod_{i=1}^{r}(1 - t^r)$. For $\lambda = (\lambda_1, \lambda_2, \cdots, \lambda_k) \vdash n$, where each λ_i appears m_{λ_i} times, set $\phi_\lambda(t) := \prod_{i=1}^{k} \phi_{m_{\lambda_i}}(t)$.
- Also if λ' is the *conjugate partition* of λ, let $n(\lambda) = \sum_{i=1}^{l(\lambda')} \frac{\lambda'_i(\lambda'_i - 1)}{2}$.
- Now if $A \in c = (\{z_i\}, \{d_i\}, \{\nu_i\}, \{f_i\})$, then by Green [2], we have

Size of Conjugacy Classes of $GL(n, q)$

$$|C_{GL(n,q)}(A)| = \prod_{i=1}^{k} q^{d_i(z_i+2n(\nu_i))}\phi_{\nu_i}(q^{-d_i}). \tag{1}$$

It follows that

$$|C_A| = (\prod_{s=0}^{n-1}(q^n - q^s))/\prod_{i=1}^{k} q^{d_i(z_i+2n(\nu_i))}\phi_{\nu_i}(q^{-d_i}). \tag{2}$$

Number of Regular Semisimple Elements of $GL(n,q)$

Counting the number of the regular semisimple elements of $GL(n,q)$ relies on

- calculating the number of regular semisimple types,
- calculating the number of classes contained in each of the regular semisimple types,
- calculating the number of elements contained in each of the regular semisimple classes.

Number of Regular Semisimple Types

Proposition 3

There is a $1-1$ *correspondence between the types of classes of regular semisimple elements of* $GL(n,q)$ *and partitions of* n*.*

PROOF. A regular semisimple class of $GL(n,q)$ must have the form $c=(\{f_i\},\{d_i\},\{1\}_{k\text{ times}},\{1\}_{k\text{ times}})$. Thus all regular semisimple classes of the same type define the partition $(d_1,d_2,\cdots,d_k)\vdash n$. Conversely, it is easy to show that any partition $\lambda=(\lambda_1,\lambda_2,\cdots,\lambda_k)\vdash n$ defines a type of regular semisimple classes, where a typical class c will have the form $c=(\{f_i\},\{\lambda_i\},\{1\}_{k\text{ times}},\{1\}_{k\text{ times}}),\ 1\leq i\leq k$. Hence the result. ∎

Number of Regular Semisimple Classes of $GL(n, q)$

- It turns out that we may denote any type of regular semisimple classes of $GL(n, q)$ by $\mathcal{T}^{\lambda}$ and a typical class by c^{λ} without any ambiguity.
- Consider the other representation of any partition $\lambda = (\lambda_1, \lambda_2, \cdots, \lambda_k) \vdash n$ namely $\lambda = (1^{r_1} 2^{r_2} \cdots n^{r_n}) \vdash n$, where $r_i \in \mathbb{N} \cup \{0\}$.
- Recall that by a result of Gauss (see Lidl and Niederreiter [3]), the number of irreducible polynomials of degree i over $\mathbb{F}_q$ is given by $I_i(q) = \frac{1}{i} \sum_{d|i} \mu(d) q^{\frac{i}{d}}$, where μ is the *Möbuis function*.

Number of Regular Semisimple Classes of $GL(n, q)$

Proposition 4

The number of regular semisimple classes of type λ, which we denote by $F(\lambda)$, is given by

$$F(\lambda) = \left(\prod_{i=1}^{n} \prod_{s=0}^{r_i - 1} (l_i(q) - s) \right) \Big/ \left(\prod_{i=1}^{n} r_i! \right),$$

where if $r_i - 1 < 0$, then the term $\prod_{s=0}^{r_i-1} (l_i(q) - s)$ is neglected.

PROOF. See Proposition 5 Moori and Basheer [4]. ∎

Number of Regular Semisimple Elements of $GL(n,q)$

Proposition 5

Let c^{λ} be a regular semisimple class, where $\lambda=(\lambda_1,\lambda_2,\cdots,\lambda_k)\vdash n$. Then

$$|c^{\lambda}| = \left(\prod_{s=0}^{n-1}(q^n-q^s)\right) \Big/ \left(\prod_{i=1}^{k}(q^{\lambda_i}-1)\right).$$

PROOF. Let $g\in c^{\lambda}=(\{f_i\},\{\lambda_i\},\{1\}_{k\text{ times}},\{1\}_{k\text{ times}})$. Since $\nu_i=1,\ \forall 1\le i\le k$, we obtain by substituting in equation (1) that

$$|C_{GL(n,q)}(g)| \;=\; \prod_{i=1}^{k} q^{\lambda_i}\phi_1(q^{-\lambda_i}) = \prod_{i=1}^{k} q^{\lambda_i}\left(\frac{q^{\lambda_i}-1}{q^{\lambda_i}}\right) = \prod_{i=1}^{k}(q^{\lambda_i}-1).$$

The result follows by equation (2). ■

Some Corollaries (Moori and Basheer [4])

- For any positive integer n, two partitions namely, $\lambda = \underbrace{(1, 1, \cdots, 1)}_{n \text{ times}} \vdash n$ and $\sigma = (n) \vdash n$ are of particular interest.
- With $q > n$, we have $F(\lambda) = \frac{(q-1)(q-2)\cdots(q-n)}{n!}$ and $F(\sigma) = \frac{1}{n}\sum_{d|n} \mu(d) q^{\frac{n}{d}}$.
- We have $|c^{\lambda}| = q^{\frac{n(n-1)}{2}} \prod_{i=1}^{n-1} \sum_{j=0}^{i} q^j$ and $|c^{\sigma}| = q^{\frac{n(n-1)}{2}} \prod_{i=1}^{n-1} (q^i - 1)$.

The Main Theorem: Number of Regular Semisimple Elements of $GL(n,q)$

Theorem 6

With $\lambda = (\lambda_1, \lambda_2, \cdots, \lambda_k) \equiv 1^{r_1} 2^{r_2} \cdots n^{r_n}$ for $r_i \in \mathbb{N} \cup \{0\}$, the number of regular semisimple elements of $GL(n,q)$ is given by

$$\sum_{\lambda \vdash n} \frac{\prod_{s=0}^{n-1}(q^n - q^s) \prod_{i=1}^{n} \prod_{s=0}^{r_i - 1} (I_i(q) - s)}{\prod_{i=1}^{k}(q^{\lambda_i} - 1) \prod_{i=1}^{n} r_i!}.$$

PROOF. Follows from Propositions 3, 4 and 5. ∎

Example

- Consider $GL(4, q)$. Corresponds to $(2, 2) = 2^2 \vdash 4$, we have

$$F(2^2) = \left(\prod_{i=1}^{4}\prod_{s=0}^{r_i-1}(l_i(q) - s)\right) \Big/ \left(\prod_{i=1}^{n} r_i!\right) = \frac{q(q^2-1)(q-2)}{8}.$$

$$|c^{(2,2)}| = \frac{\prod_{s=0}^{3}(q^4 - q^s)}{\prod_{i=1}^{2}(q^{\lambda_i} - 1)} = q^6(q-1)(q^2+1)(q^3-1).$$

- Hence there are $\frac{q^7(q^4-1)(q^3-1)(q-1)(q-2)}{8}$ regular semisimple elements of type $(2, 2)$.

Example

- Repeating the previous work to the other four partitions of 4, we get a total number of regular semisimple elements of $GL(4, q)$ given by

$$q^{16} - 2q^{15} + q^{13} + q^{12} - 2q^{10} - q^9 - q^8 + 2q^7 + q^6.$$

- For example the group $GL(4, 5)$, which is of order 116,064,000,000 has 9,299,587,000 regular semisimple elements.
- In Table 2 of Moori and Basheer [4] we list the number of types, conjugacy classes, elements in each conjugacy class of regular semisimple elements of $GL(n, q)$ for $n = 1, 2, 3, 4, 5, 6$.
- The number of regular semisimple elements of $GL(n, q)$ for $n = 1, 2, 3, 4, 5, 6$ is an integral polynomial in q.

Number of Primary Classes of $GL(n, q)$

- Recall that a class $c = (\{f_i\}, \{d_i\}, \{z_i\}, \{\nu_i\})$ of $GL(n, q)$ with length k is primary if and only if $k = 1$. That is $c = (f, d, \frac{n}{d}, \nu)$ for some $f \in \mathcal{F}_{\leq n}$ with degree d, $d|n$, and $\nu \vdash \frac{n}{d}$.

Theorem 7

The number of primary classes $pc(n, q)$ of $GL(n, q)$ is given by

$$pc(n, q) = \sum_{d|n} |\mathcal{P}(\frac{n}{d})| \cdot I_d(q), \text{ where } \mathcal{P}(j) \text{ is the set partitions of } j.$$

PROOF. For fixed d and any $\nu \vdash \frac{n}{d}$ we have $I_d(q)$ irreducible polynomials f of degree d, that defines a primary class. Hence there are $|\mathcal{P}(\frac{n}{d})| \cdot I_d(q)$ classes defined by the fixed integer d and partitions of $\frac{n}{d}$. The result follows by letting d runs over all divisors of n. ∎

$pc(n, q)$ for $n = 1, 2, \cdots, 6$ and any q

Table: Number of primary classes of $GL(n, q)$, $n = 1, 2, 3, 4, 5, 6$.

n	$pc(n, q)$
1	$(q - 1)$
2	$(q^2 + 3q - 4)/2$
3	$(q^3 + 8q - 9)/3$
4	$(q^4 + 3q^2 + 16q - 20)/4$
5	$(q^5 + 34q - 35)/5$
6	$(q^6 + 3q^3 + 8q^2 + 54q - 66)/6$

Some Corollaries (Moori and Basheer [4])

- There are exactly $I_n(q) = \frac{1}{n}\sum_{d|n} \mu(d)q^{\frac{n}{d}}$ primary regular semisimple classes of $GL(n, q)$.
- If $n = p^{'}$ is a prime integer (whether $p^{'} = p$, the characteristic of $\mathbb{F}_q$ or not), then there are $I_{p'}(q) = \frac{q^{p^{'}} - q}{p^{'}}$ primary regular semisimple classes of $GL(p^{'}, q)$.
- We have $\left[q^{\frac{p^{'2} - p^{'} + 2}{2}} (q^{p^{'}} - 1)^2 \prod_{i=1}^{p^{'}-2} (q^i - 1) \right] \Big/ p^{'}$ primary regular semisimple elements of $GL(p^{'}, q)$.
- The group $GL(p^{'}, q)$ has exactly $(q^{p^{'}} + (p^{'}|\mathcal{P}(p^{'})| - 1)q - p^{'}|\mathcal{P}(p^{'})|)/p^{'}$ primary conjugacy classes.

The Bibliography

- A. B. M. Basheer, *Character Tables of the General Linear Group and Some of its Subroups*, MSc Dissertation, University of KwaZulu Natal, Pietermaritzburg, 2009.
- J. A. Green, *The characters of the finite general linear groups*, American Mathematical Society, **80** (1956), 402 - 447.
- R. Lidl and H. Niederreiter, *Finite fields*, Encyclopedia of mathematics and its application, Cambridge University Press, 1997.
- J. Moori and A. B. M. Basheer, *On the regular semisimple elements and primary classes of* $GL(n, q)$, In preparation 2009.
- J. J. Rotman, *An Introduction to the Theory of Groups*, 4^{th} edition, Springer-Verlag New York, Graduate Texts in Mathematics, **148**, 1995.

Acknowledgement

My special thanks and regards addressed to

- my supervisor Professor Jamshid Moori.
- National Research Foundation (NRF) (Prof. Moori's research grant) and to the African Institute for Mathematical Sciences (AIMS) for the grant holder bursaries.
- Administration of the University of Khartoum (UofK), in particular the Faculty of Mathematical Sciences and to the Principal of UofK, Dr Mohsin H. A. Hashim, Khartoum, Sudan.
- The University of KwaZulu Natal.