The Expected Order of a Random Unitary Matrix
(Preliminary Version)

Eric Schmutz
Department of Mathematics
Drexel University
Philadelphia, Pa. 19104
Eric.Jonathan.Schmutz@drexel.edu
March 11, 2021

Abstract

Let $U(n, q)$ be the group consisting of those invertible matrices $A = (a_{i,j})_{1 \leq i,j \leq n}$ whose inverse is the conjugate transpose with respect to the involution $c \mapsto c^q$ of the finite field $F_{q^2}$. In other words, the $i,j$'th entry of $A^{-1}$ is $a_{j,i}^q$. Let $\mu_n = \frac{1}{|U(n,q)|} \sum_{A \in U(n,q)} \text{Order}(A)$ be the average of the orders of the elements in this finite group. We prove the following conjecture of Fulman: for any fixed $q$, as $n \to \infty$,

$$\log \mu_n = n \log(q) - \log n + o_q(\log n).$$

Keywords and phrases: Unitary group, finite field, cycle index
1 Introduction

This paper concerns the finite unitary group $U(n,q)$, so we begin by reviewing some basic notation and definitions relating to this group. Let $q = p^\ell$ for some prime number $p$ and some positive integer $\ell$. The involution $c \mapsto c^q$ is an automorphism of the finite field $F_{q^2}$ that fixes the subfield $F_q$. If $A = (a_{i,j})_{1 \leq i,j \leq n}$ is an $n \times n$ matrix with entries in $F_{q^2}$, let $A^\ast$ be the matrix whose $i,j$'th entry is $a_{j,i}^q$ (for $1 \leq i, j \leq n$). Define the unitary group $U(n,q)$ to be the group consisting of those $n \times n$ matrices $A$ for which $A^{-1} = A^\ast$. It is well known (e.g.\cite{5}, page 109) that, under matrix multiplication, this set of matrices forms a group of order

$$|U(n,q)| = q^{n^2} \prod_{j=1}^{n} (1 - \frac{(-1)^j}{q^j}). \quad (1)$$

For any prime power $r$, let $GL(n,r)$ be the group of invertible $n \times n$ matrices with entries in $F_r$. It is well known that $GL(n,r)$ has order

$$|GL(n,r)| = r^{n^2} \prod_{j=1}^{n} (1 - \frac{1}{r^j}). \quad (2)$$

Note that $U(n,q)$ is a subgroup of $GL(n,q^2)$, not $GL(n,q)$.

For any finite group $G$, let $\mu(G) = \frac{1}{|G|} \sum_{g \in G} V(g)$, where $V(g)$ is the order of $g$. Stong \cite{9} proved that, for any prime power $r$,

$$\log \mu(GL(n,r)) = n \log r - \log n + o_r(\log n). \quad (3)$$

as $n \to \infty$. Fulman proposed the analogous problem estimating $\mu(U(n,q))$. He proved that $\log \mu(U(n,q)) \geq \frac{1}{2} n \log q^2 - \log n + o_q(\log n)$, and conjectured that this lower bound is sharp insofar as the "$\geq$" can be replaced with "=". The goal of this paper is to prove Fulman’s conjecture.

The rest of this section contains additional definitions and symbols that are listed in quasi-alphabetical order, and then used globally without comment.

- $|f|$: the degree of the polynomial $f$.
- $\bar{f}$: if $f(x) = x^d + \sum_{j=0}^{d-1} a_j x^j$ is a monic polynomial of degree $d$ with non-zero constant term $a_0$, then $\bar{f}(x) = x^d + \sum_{j=0}^{d-1} a_{d-j} a_j^q x^j$.
- $[[z^n]]F(z)$: coefficient of $z^n$ in $F(z)$.
- $c_i(\pi)$: number of parts of size $i$ that the partition $\pi$ has.
- $C_\infty = \prod_{j=1}^{\infty} (1 - \frac{1}{2^j}) \approx .289$
- $E_n$: expected value with respect to $P_n$, i.e. for any real valued function $Y$ that is defined on characteristic polynomials of matrices in $U(n,q)$, $E_n(Y) = \frac{1}{|U(n,q)|} \sum_{A \in U(n,q)} Y(char.poly.(A))$. 

1
• \( I_{d,r} = \) set of all monic polynomials of degree \( d \) in \( F_r[x] \) that are irreducible over \( F_r \) (except for \( \phi(x) = x \), which is excluded from \( I_1 \)).

• \( I_d = I_{d,q^2} \)

• \( I = \bigcup_{d=1}^{\infty} I_{d,q^2} \).

• \( J_d = \) monic, irreducible polynomials \( \phi \) of degree \( d \) in \( F_{q^2}[x] \) that satisfy \( \phi = \tilde{\phi} \)

• \( J = \bigcup_{d=1}^{\infty} J_d \).

• \( K_d = I_{d,q^2} - J_d = \) monic, irreducible polynomials \( \phi \) of degree \( d \) in \( F_{q^2}[x] \) that satisfy \( \phi \neq \tilde{\phi} \)

• \( K = \bigcup_{n=1}^{\infty} K_d \).

• \( K_+, K_- : \) disjoint subsets of \( K \) such that \( \phi \in K_+ \) iff \( \tilde{\phi} \in K_- \).

• \( m_\phi = m_\phi(f) = \) the multiplicity of \( \phi \) in \( f \): for \( \phi \in I \) and \( f \in F_{q^2}[x] \), \( \phi^{m_\phi(f)} \) divides \( f \) but \( \phi^{m_\phi(f)+1} \) does not divide \( f \).

• \( m_\phi(A) = m_\phi(\text{characteristic polynomial of } A) \).

• \( M = \max_{\phi \in I} m_\phi \).

• \( Q_b = \) set of all partitions of \( b \) into distinct odd parts.

• \( \Omega_n = \) all characteristic polynomials of matrices in \( U(n,q) = \) monic, degree \( n \), polynomials \( f \in F_{q^2}[x] \) satisfying \( m_\phi(f) = m_{\tilde{\phi}}(f) \) for all \( \phi \in I \).

• \( P_n = \) the probability measure on \( \Omega_n \) that is induced by the uniform distribution on \( U(n,q) \), i.e. \( P_n(S) = \frac{|\{A \in U(n,q): \text{char.poly}(A) \in S\}|}{|U(n,q)|} \) for all \( S \subseteq \Omega_n \).

• \( Q_n = \) set of all partitions of \( n \) into distinct parts.

• \( \tau_\phi = \) order of the roots of the irreducible polynomial \( \phi \) (as multiplicative units in the splitting field for \( \phi \)).

• \( T(f) = LCM\{\tau_\phi : \phi \text{ is an in irreducible factor of } f\} \)

• \( X_1(f) = LCM(\{q^{\phi} + 1 : m_\phi(f) > 0, \phi \in J\}) \).

• \( X_2(f) = LCM(\{q^{2\phi} - 1 : m_\phi(f) > 0, \phi \in K_+\}) \).

• \( X_1(\pi) = LCM(\{q^d + 1 : \pi \text{ has a part of size } d\}) \).

• \( X_2(\lambda) = LCM(\{q^{2d} - 1 : \lambda \text{ has a part of size } d\}) \).

• \( X(f) = \) least common multiple of \( X_1(f) \) and \( X_2(f) \).

• \( X(A) = X(\text{ characteristic polynomial of } A) \).

• \( V(A) = \) order of \( A = \min\{e : A^e = I\} \).
2 Reduction from V to X

There is a close relationship between the order of a matrix $A \in GL(n, q^2)$ and the orders of its eigenvalues (as multiplicative units in a splitting field for the characteristic polynomial). Hence we begin this section with a simple lemma about the orders of the roots of irreducible polynomials. We also state, for future reference, Fulman’s formula for the number of unitary matrices with a given characteristic polynomial. These facts are used to bound the maximum order, and to prove that most matrices in $U(n, q)$ do not have eigenvalues of large algebraic multiplicity. This in turn enables us to reduce the problem of estimating $E_n(V)$ to the easier problem of estimating $E_n(X)$.

Recall that, if $\phi(x) = x^d + \sum_{j=0}^{d-1} a_j x^j$ is a monic polynomial of degree $d$ with non-zero constant term $a_0$, then $\phi(x) = x^d + \sum_{j=0}^{d-1} a_j x^j$.

Lemma 1 Suppose $\phi \in I_d$, and suppose $\tau_\phi$ and $\tau_{\tilde{\phi}}$ are respectively the orders of the roots of $\phi$ and $\tilde{\phi}$ (as multiplicative units in $\mathbb{F}_{q^2}$). Then
\begin{itemize}
  \item $\tau_\phi = \tau_{\tilde{\phi}}$
  \item If $\phi = \tilde{\phi}$, then $\tau_\phi$ is a divisor of $q^d + 1$.
\end{itemize}

Proof: Observe that $\rho$ is a root of $\phi$ if and only if $\rho^{-q}$ is a root of $\tilde{\phi}$:
\begin{align}
\tilde{\phi}(\rho^{-q}) &= a_0^{-q} \rho^{-dq} \sum_{k=0}^{d} a_k \rho^{kq} \\
&= a_0^{-q} \rho^{-dq} \left( \sum_{k=0}^{d} a_k \rho^{k} \right)^q.
\end{align}

As an element of $\mathbb{F}_{q^2}^*$, the order of $\rho^{-q}$ is equal to the order of its inverse $\rho^d$, which is in turn equal to the order of $\rho$ (since $q$ and $q^{2d} - 1$ are coprime). This proves the first part: $\tau_\phi = \tau_{\tilde{\phi}}$.

Let $\rho$ be one of the roots of $\phi$, assume that $\phi = \tilde{\phi}$. Then $\rho^{-q}$ must be one of the roots of $\phi$. But the roots of $\phi$ are $\rho^2, \rho^q, \ldots, \rho^{q^{2d-2}}, \rho^{2d} = \rho$. Hence, for some positive integer $j \leq d$, we have $\rho^{dq} = \rho^{-q}$, and consequently $\rho^q = 1$. This proves that $\tau_\phi$ divides $q(q^{2j-1} + 1)$. But $\tau_\phi$ also divides $q^{2d} - 1$, and $\gcd(q, q^{2d} - 1) = 1$. Therefore $\tau_\phi$ divides $q^{2j-1} + 1$. Let $m$ be the smallest positive integer such that $\tau_\phi$ divides $q^m + 1$. If $\tau_\phi = 2$, then it is clear that $\tau_\phi$ divides $q^d + 1$ since $\tau_\phi$ divides $q^d - 1 = (q^d + 1)(q^d - 1)$ and both factors are even. We may therefore assume that $\tau_\phi > 2$. Using Proposition 1 of [11] (with $s = 2d$), and the fact that $\tau_\phi | q^{2d} - 1$, we get $2d = 2\ell n$ for some positive integer $\ell$. We know $d$ is odd (Fulman [2], Theorem 9), therefore $\ell$ must also be odd. Again using Proposition 1 of [11] (this time with $s = d$), we get $\tau_\phi | q^d + 1$. □
Let $\Omega_n$ be the set of polynomials that are characteristic polynomials of matrices in $U(n,q)$. A beautiful characterization of these polynomials is known. A monic polynomial $f$ is in $\Omega_n$ if and only if $m_\phi(f) = m_\tilde{\phi}(f)$ for all $\phi \in \mathcal{I}$; the multiplicity of $\phi$ is the same as the multiplicity of $\tilde{\phi}$ for all irreducible polynomials $\phi$. In fact, with the notational convention that $|U(0,r)| = |GL(0,r)| = 1$ for all prime powers $r$, we can state the following theorem of Fulman\[2]:

**Theorem 2** (Fulman) If $f \in \Omega_n$, then

$$P_n(\{f\}) = \prod_{\phi \in \mathcal{J}} \frac{q^{\phi(m_2^\phi - m_\phi)}}{|U(m_\phi, q^{\phi})|} \cdot \prod_{\phi \in \mathcal{K}_+} \frac{q^{2|\phi|(m_2^\phi - m_\phi)}}{|GL(m_\phi, q^{2|\phi|})|}$$

Theorem\[2] was just one application of powerful generating function techniques that Fulman developed for $U(n,q)$ and other finite classical groups. Related work can be found in Kung\[6], Stong\[10], and recent work of Fulman, Neumann, and Praeger, e.g. \[3].

If the eigenvalues are all distinct, then the order of a matrix is just the least common multiple of the orders of the eigenvalues. The general case is a bit more complicated because the Jordan form includes off-diagonal elements. This leads to Theorem 3 below. This convenient inequality is an immediate consequence of the slightly stronger inequality in the introduction of Stong’s paper \[9]. (See also Lidl and Niederreiter\[7], page 80):

**Theorem 3** For all $A \in GL(n,q^2)$, $V \leq pMT$.

An immediate consequence of Theorem 3 is a bound on the maximum order:

**Corollary 4** For all $A \in GL(n,q^2)$, $V < pqn^2$.

However a stronger inequality holds for $U(n,q)$.

**Corollary 5** For all $A \in U(n,q)$, $V \leq 3pMq^n$.

**Proof:** By Theorem 3 it suffices to prove that $T \leq 3q^n$. Suppose the characteristic polynomial of $A$ is

$$\prod_{i=1}^r \phi_i^{m_{\phi_i}} \prod_{j=1}^s (\phi_{r+j} \tilde{\phi}_{r+j})^{m_{\phi_{r+j}}}$$

where $\phi_i \in \mathcal{J}$ for $i \leq r$ and $\phi_{r+j} \in \mathcal{K}_+$ for $j \leq s$. To simplify notation, let $d_i = |\phi_i|$, and $\tau_i = \tau_{\phi_i}$. Then by Lemma 11, $\tau_i$ divides $(q^{d_i} + 1)$ for $i \leq r$ and $\tau_i$ divides $q^{2d_i} - 1$ for $r < i \leq r + s$. Hence

$$T(A) = LCM(\tau_1, \tau_2 \ldots \tau_{r+s}) \leq \cdot LCM(q^{d_1} + 1, q^{d_2} + 1) \ldots q^{d_r} + 1)LCM(q^{2d_{r+1}} - 1, \ldots , q^{2d_{r+s}} - 1)$$

(6)

(7)
Without loss of generality, assume $d_i \neq d_j$ for $1 \leq i < j \leq r$. (If two degrees are equal, then we can remove one of the arguments to the least common multiple function without changing its value.) Then

\[ T(A) \leq \prod_{i=1}^{r} (q^{d_i} + 1) \cdot \prod_{j=1}^{n} q^{2d_{r+j}} \tag{8} \]

\[ = q^n \prod_{i=1}^{r} (1 + 1/q^{d_i}) \tag{9} \]

\[ \leq q^n \prod_{i=1}^{r} (1 + 1/2i) \leq 3q^n. \tag{10} \]

\[ \square \]

We have a bound on the maximum order, but we still need to prove that the maximum multiplicity $M$ is usually small. If $\xi = \xi(n) \to \infty$, then with high probability, no irreducible factor has multiplicity larger than $\xi$.

**Lemma 6** For all positive integers $n$, and all $\xi > 2$, $P_n(M > \xi) \leq 40q^{-1-\xi}$.

**Proof:** Suppose $d$ is a positive integer $\leq n$ and $\psi = \tilde{\psi} \in J_d$. Note that, for $f \in \Omega_n$, we have $m_\psi(f) = \ell$ if and only if $f = \psi^\ell g$ for some $g \in \Omega_{n-\ell}$ such that $m_\psi(g) = 0$. Hence, by Theorem 2

\[ P_n(m_\psi = \ell) = \frac{q^{d\ell^2-d\ell}}{|U(\ell, q^d)|} P_n(\ell, q^d|) \leq \frac{q^{d\ell^2-d\ell}}{|U(\ell, q^d)|}. \tag{11} \]

Using (1), we get

\[ \frac{q^{d\ell^2}}{|U(\ell, q^d)|} = \frac{1}{\ell \prod_{j=1}^{\ell} (1 - (-1)^{j}/q^{d_j})} \]

\[ < \frac{1}{\ell \prod_{j=1}^{\ell} (1 - 1/q^{d_j})} < \frac{1}{C_\infty} < 4. \tag{14} \]

Putting this back into the right side of (11), and summing on $\ell$, we get

\[ P_n(m_\psi \geq \xi) = \sum_{\ell \geq \xi} P_n(m_\psi = \ell) \leq 4 \sum_{\ell \geq \xi} q^{-\ell d} \leq 8q^{-d\xi}. \tag{16} \]

5
Similarly, for any $\psi \in K_d$, we have
\begin{align*}
P_n(m_\psi = \ell) &= \frac{q^{2d(\ell^2 - \ell)}}{|GL(\ell, q^{2d})|} P_{n-2d}(m_\psi = 0) \\
&\leq \frac{q^{2d(\ell^2 - \ell)}}{|GL(\ell, q^{2d})|} = \ell \prod_{j=1}^{\ell} \left(1 - \frac{1}{q^{2d}}\right) \\
&< \frac{q^{-2\ell}}{\prod_{j=1}^{\infty} \left(1 - \frac{1}{2^{2j}}\right)} < 2q^{-2\ell},
\end{align*}
and consequently
\begin{equation}
P_n(m_\psi \geq \xi) \leq 4q^{-2\ell}. \tag{21}
\end{equation}

Now, given a real number $\xi > 2$, let $N_\xi$ be the number of irreducible factors having multiplicity greater than $\xi$. Then $M > \xi$ if and only if $N_\xi > 0$, and it suffices to show that $P_n(N_\xi > 0) \leq 40q^{1-\xi}$.

Combining (16) and (21), we get
\begin{align*}
P_n(N_\xi > 0) &\leq E(N_\xi) = \sum_{d=1}^{\lfloor n/d\xi \rfloor} \sum_{\phi \in I_d, \phi \neq \ell} P_n(m_\phi > \xi) \\
&= \sum_{d=1}^{\lfloor n/d\xi \rfloor} \left( \sum_{\phi \in J_d} P_n(m_\phi > \xi) + \sum_{\phi \in K_d} P_n(m_\phi > \xi) \right) \\
&\leq \sum_{d=1}^{\infty} \left( |J_d|q^{-d\xi} + |K_d|4q^{-2d\xi} \right). \tag{24}
\end{align*}

It is well known (e.g. [1], page 80) that, for any prime power $r$,
\begin{equation}
|I_{d,r}| = \frac{1}{d} \sum_{k|d} \mu(k) r^{d/k} \leq \frac{r^d}{d} \tag{25}
\end{equation}
Since $K_d \subseteq I_{d,q^2}$, we follows that
\begin{equation}
|K_d| \leq \frac{q^{2d}}{d}. \tag{26}
\end{equation}

We need a similar estimate for $|J_d|$. Fulman proved that
\begin{equation}
|J_d| = \begin{cases} 
0 & \text{if } d \text{ is even}, \\
\frac{1}{d} \sum_{k|d} \mu(k)(q^{d/k} + 1) & \text{else.}
\end{cases} \tag{27}
\end{equation}
It is well known that, for all \( d > 1 \), \( \sum_{k|d} \mu(k) = 0 \). Therefore, for all odd \( d > 1 \),
\[
|J_d| = \frac{1}{d} \sum_{k|d} \mu(k) q^{d/k} = |I_{d,q}| \leq \frac{q^d}{d}.
\] (28)

(It is interesting that \( |J_d| \) is exactly equal to \( |I_{d,q}| \), even though the two sets are not equal.) For \( d = 1 \) we have \( |J_d| = q + 1 \leq 2q \), so for all \( d \geq 1 \) we crudely have
\[
|J_d| \leq \frac{2q^d}{d}.
\] (29)

For \( 0 < x < \frac{1}{2} \), we have \(-\log(1-x) < 2x\), and for \( \xi > 2 \), we have \( q^{1-\xi} < \frac{1}{2} \).

Therefore, by putting (29) and (26) into (24), we get
\[
P_n(N_\xi > 0) \leq \sum_{d=1}^{\infty} \left( \frac{16q^{d-\xi}}{d} + \frac{4q^{2d-2d\xi}}{d} \right)
\]
\[
\leq -20 \log(1 - q^{1-\xi}) \leq 40q^{1-\xi}.
\] (31)

\[\blacksquare\]

Now that Lemma 6 is available, we can reduce the problem from the task of estimating \( E_n(V) \) to the slightly easier task of estimating \( E_n(X) \).

**Lemma 7** \( \log E_n(V) \leq \log E_n(X) + O(\log \log n) \).

**Proof:** By lemma 1, \( T(A) \) divides \( X(A) \) for all \( A \). It therefore suffices to prove that
\[
\log E_n(V) \leq \log E_n(T) + O_p(\log \log n).
\] (32)

For any \( \xi \), we have
\[
E_n(V) = P_n(M \leq \xi) E_n(V|M \leq \xi) + P_n(M > \xi) E_n(V|M > \xi).
\] (33)

To estimate the second term of the two terms on the right side of in (33), we use Corollary 5 and Lemma 6 with \( \xi = \log^2 n \):
\[
P_n(M > \xi) E_n(V|M > \xi) \leq (40q^{1-\log^2 n})(3pnq^n) = q^n(1+o(1)).
\] (34)

For the first term on the right side of (33), we are conditioning on \( M \leq \xi \) so we can use the inequality \( M \leq \xi \) together with the inequality \( V \leq pMT \) from Theorem 6
\[
P_n(M \leq \xi) E_n(V|M \leq \xi) \leq p\xi P_n(M \leq \xi) E_n(T|M \leq \xi)
\]
\[
\leq p\xi (P_n(M \leq \xi) E_n(T|M \leq \xi) + P_n(M > \xi) E_n(T|M > \xi))
\]
\[
= p\xi E_n(T).
\] (38)
Finally, putting (38) and (34) back into (33), we get
\[ E_n(\mathbf{V}) \leq (p \log^2 n) E_n(\mathbf{T}) \left( 1 + \frac{q^{n-\log n}(1+o(1))}{E_n(\mathbf{T})} \right). \] (39)

Since \( E_n(\mathbf{T}) \geq q^{n-\log n} \) for all sufficiently large \( n \) (section 6 of Fulman [2]), the lemma follows from (39) by taking logarithms. \( \square \)

3 Key Factorization.

There is a second factorization of characteristic polynomials that is crucial for this paper. The idea is to factor the characteristic polynomial \( f \) as \( f = gh \) where
- \( \mathbf{X}(f) = \mathbf{X}(g) \)
- \( g \) is easier to work with than \( f \), and
- \( g \) and \( h \) are themselves characteristic polynomials of unitary matrices.

To that end, define \( \mathcal{D}(f) \) to be the set of polynomials \( g \) that satisfy the following three conditions:
- \( g \in \Omega \)
- \( g \) divides \( f \)
- \( \mathbf{X}(g) = \mathbf{X}(f) \)

The set \( \mathcal{D}(f) \) is non-empty since \( f \in \mathcal{D}(f) \). Because \( \mathcal{D}(f) \) is a non-empty finite set that is partially ordered by divisibility, we can choose a minimal element \( \pi(f) \).

Suppose we have chosen, for each \( f \in \Omega_n \), a factor \( g = \pi(f) \) that is minimal in \( \mathcal{D}(f) \). It is clear that, no matter how the minimal element is chosen, it will have the following useful properties:
- For all \( \phi \) in \( \mathcal{I} \), \( m_{\phi}(g) = 0 \) or 1.
- For all positive integers \( d \), \( \pi(f) \) has zero, one, or two irreducible factors of degree \( d \). If there is one such irreducible factor \( \phi \), then \( \phi \in \mathcal{J}_d \). If there are two, and \( \phi \) is one of them, then \( \phi \) is the other and both are in \( \mathcal{K}_d \).

The third property we need is less obvious, but it is proved in the following lemma.

Lemma 8 If \( f \in \Omega_n \) and \( g = \pi(f) \) has degree \( |g| < n \), and if \( h = \frac{f}{\pi(f)} \), then
\[ P_n(\{f\}) \leq P_{|g|}(\{g\}) P_{n-|g|}(\{h\}). \]

Proof: We consider each factor of \( P_n(\{f\}) \) in the factorization of Theorem 2 and show that it is bounded above by the corresponding factors in the product \( P_{|g|}(\{g\}) P_{|h|}(\{h\}) \).

8
Suppose first that \( \phi \in J_d \) for some \( d \), and suppose \( \phi \) divides \( g \). To simplify notation, let \( m = m_\phi(f) \). In Theorem 2, the factor of \( P_n(\{f\}) \) corresponding to \( \phi \) is

\[
\frac{q^{d(m^2-m)}}{|U(m, q^d)|} = \frac{q^{-dm}}{\prod_{j=1}^{m} \left( 1 - \frac{(-1)^j}{q^{dm}} \right)}
\]

(40)

\[
= \frac{q^{-d}}{(1 - \frac{(-1)^m}{q^{dm}})} \frac{q^{-d(m-1)}}{\prod_{j=1}^{m-1} \left( 1 - \frac{(-1)^j}{q^{dm}} \right)}
\]

(41)

\[
\leq \frac{q^{-d}}{(1 - \frac{1}{q^d})} \frac{q^{-d(m-1)}}{\prod_{j=1}^{m-1} \left( 1 - \frac{(-1)^j}{q^{dm}} \right)}
\]

(42)

Since \( \phi \) divides \( g \), we have \( m_\phi(g) = 1 \) and \( m_\phi(h) = m - 1 \). Therefore the factor of \( P_{|g|}(g) \) that corresponds to \( \phi \) is \( q^{-d} \frac{q^{-d(m-1)}}{(1 - \frac{(-1)^d}{q^{dm}})} \), and the factor of \( P_{|h|}(h) \) that corresponds to \( \phi \) is \( \frac{q^{-d(m-1)}}{\prod_{j=1}^{m-1} \left( 1 - \frac{(-1)^j}{q^{dm}} \right)} \). These are precisely the two factors on the right side of (42).

Similarly, if \( \phi \in K^+ \) has degree \( d \) and \( \phi \) divides \( g \), then the factor of \( P_n(\{f\}) \) that corresponds to \( \phi \) is

\[
\frac{q^{2d(m^2-m)}}{|GL(m, q^{2d})|} = \frac{q^{-2dm}}{\prod_{j=1}^{m} \left( 1 - \frac{1}{q^{2dm}} \right)}
\]

(43)

\[
\leq \frac{q^{-2d}}{(1 - \frac{1}{q^{2d}})} \frac{q^{-2d(m-1)}}{\prod_{j=1}^{m-1} \left( 1 - \frac{1}{q^{2dm}} \right)}
\]

(44)

Again \( m_\phi(g) = 1 \) and the factor of \( P_{|g|}(g) \) that corresponds to \( \phi \) is \( q^{-2d} \frac{q^{-2d(m-1)}}{(1 - \frac{1}{q^{2dm}})} \). Likewise \( m_\phi(h) = m - 1 \), and the factor of \( P_{|h|}(h) \) that corresponds to \( \phi \) is \( \frac{q^{-2d(m-1)}}{\prod_{j=1}^{m-1} \left( 1 - \frac{1}{q^{2dm}} \right)} \). Again these two expressions are precisely factors on the right side of (44).

Finally, if \( \phi \) does not divide \( g \), then \( m_\phi(g) = 0 \) and \( m_\phi(f) = m_\phi(h) \). In this case, the factor of \( P_{|g|}(g) \) that corresponds to \( \phi \) is 1, and the factor of \( P_{|h|}(h) \) that corresponds to \( \phi \) is exactly the same as the factor \( P_n(\{f\}) \) that corresponds to \( \phi \).

\[ \square \]
4 Estimating $E_n(X)$.

We know have all the tools necessary to prove the main result:

**Theorem 9** \( \log E_n(V) = n \log q - \log n + o_q(\log n) \).

**Proof:** By Corollary 7 it suffices to prove that \( \log E_n(X) = n \log q - \log n + o_q(\log n) \). Recall the factorizations \( f = \pi(f)h \), and define \( G_n = \{ g : g = \pi(f) \text{ for some } f \in \Omega_n \} \). Then

\[
E_n(X) = \sum_{f \in \Omega_n} X(\{f\}) P_n(\{f\})
\]

(45)

\[
= \sum_{g \in \mathcal{V}_n} X(\{g\}) \sum_{\{h : \pi(gh) = g\}} P_n(gh).
\]

(46)

By Lemma 8, this is less than or equal to

\[
\sum_{g \in \mathcal{V}_n} X(\{g\}) P_{|g|}(\{g\}) \sum_{\{h : h = f/g \text{ for some } g \in \mathcal{V}_n\}} P_{|f/g|}(\{h\}).
\]

(47)

The inner sum is bounded by 1 since \( P_{|f/g|} \) is a probability measure. Hence

\[
E_n(X) \leq \sum_{g \in \mathcal{V}_n} X(\{g\}) P_{|g|}(\{g\}).
\]

(48)

To estimate the sum in (48), we need an upper bound for \( P_{|g|}(\{g\}) \). Note that \( |U(1, q^d)| = q^d + 1 \) and \( |GL(1, q^{2d})| = q^{2d} - 1 \) for all \( d \). Recall that, for \( g \in \mathcal{G}_n \), we have \( m_\phi(g) \leq 1 \) for all \( \phi \in \mathcal{I} \). Therefore, by Theorem 2 we have

\[
P_{|g|}(\{g\}) = q^{-|g|} \prod_{\phi \in \mathcal{J} : m_\phi(g) = 1} \frac{1}{1 + \frac{1}{q^{|\phi|}}} \prod_{\theta \in \mathcal{K} : m_\theta(g) = 1} \frac{1}{1 - \frac{1}{q^{|\theta|}}}.
\]

(49)

\[
\leq q^{-|g|} \prod_{d=1}^{\infty} \frac{1}{1 - \frac{1}{q^{|g|}}} \leq 2q^{-|g|}.
\]

(50)

Thus

\[
E_n(X) \leq 2 \sum_{g \in \mathcal{G}_n} q^{-|g|} X(\{g\}) = 2 \sum_{m=1}^{n} q^{-m} \sum_{\{g \in \mathcal{V}_n : |g| = m\}} X(g).
\]

(52)

Factor each \( g \in \mathcal{G}_n \) as \( g = g_1g_2 \), where \( g_1 \) and \( g_2 \) respectively are the products of the irreducible factors in \( \mathcal{J} \) and \( \mathcal{K} \):

\[
g_1 = \prod_{\phi \in \mathcal{J} : m_\phi(g) = 1} \phi
\]

(53)

\[
g_2 = \prod_{\theta \in \mathcal{K} : m_\theta(g) = 1} \theta \tilde{\theta}.
\]

(54)
We certainly have
\[ X(g) = LCM(X_1(g_1), X_2(g_2)) \leq X_1(g_1)X_2(g_2), \quad (55) \]
so
\[ E_n(X) \leq 2 \sum_{m=1}^{n} q^{-m} \sum_{|g| = m} X_1(g_1)X_2(g_2). \quad (56) \]
The degrees of the irreducible factors of \( g_1 \) form a partition of the integer \( |g_1| \) into distinct odd parts. Let \( S_1(\pi) \) be the set of \( g_1 \)'s with partition \( \pi \). Similarly, the degrees of the factors of \( g_2 \) from \( \theta \in K_+ \) form a partition of \( s = \frac{|g_2|}{\pi} \) into distinct parts, and we let \( S_2(\lambda) \) be the set of \( g_2 \)'s with partition \( \lambda \). Using the notation \( Q_s \) for the set of all partitions of \( s \) into distinct parts, and \( O_b \) for the set of all partitions of \( b \) into distinct odd parts, we get
\[ \sum_{\{g \in G_n : |g| = m\}} X_1(g_1)X_2(g_2) = \sum_{s=1}^{[m/2]} \pi_1 \pi_2 \ldots |S_1(\pi)||S_2(\lambda)|X_1(\pi)X_2(\lambda). \quad (57) \]
Using the inequalities (58) and (59), we get
\[ |S_1(\pi)| \leq \frac{q^{[\pi]}}{\pi_1 \pi_2 \ldots} \quad (58) \]
and
\[ |S_2(\lambda)| \leq \frac{q^{[\lambda]}}{\lambda_1 \lambda_2 \ldots} \quad (59) \]
(where \( \pi_1, \pi_2, \ldots \) are the parts of \( \pi \) and similarly for \( \lambda \)). Putting (58), (59), and (60) back into the right side of (56), we get
\[ E_n(X) \leq 2 \sum_{m=1}^{n} \left( \sum_{s=1}^{[m/2]} \sum_{\pi \in O_{m-2s}} \sum_{\lambda \in Q_s} X_1(\pi)X_2(\lambda) \right). \quad (60) \]
Let \( \sigma_2(s) = \sum_{\lambda \in Q_s} \frac{X_2(\lambda)}{\lambda_1 \lambda_2 \ldots} \) be the innermost sum. This sum was estimated by Stong at the end of [11]. The conclusion was that, as \( s \to \infty \),
\[ \sigma_2(s) \leq \frac{(q^2)^{s+o(\log s)}}{s}. \quad (61) \]
For any positive integer \( b \) define \( \sigma_1(b) = \sum_{\pi \in O_b} \frac{X_1(\pi)}{\pi_1 \pi_2 \ldots} \). We show next that it is sufficient to prove that
\[ \sigma_1(b) \leq \frac{q^{b+o(\log b)}}{b}. \quad (62) \]
Assume for now that (62) holds. (It will be verified afterwards.) For integers \( k \) let \((k)^+ = \max(k, 1)\). Use the partial fraction decomposition \( \frac{1}{s(m-2s)} = \frac{1}{ms} + \frac{2}{m(m-2s)} \) so that

\[
\sum_{s=1}^{\lfloor m/2 \rfloor} \frac{1}{s} \frac{1}{(m-2s)^+} = O\left( \frac{\log m}{m} \right).
\]

(63)

Then inside the parentheses of (60) we have

\[
\sum_{s=1}^{\lfloor m/2 \rfloor} \sigma_1(m-2s)\sigma_2(s) =
\sum_{s=1}^{\lfloor m/2 \rfloor} \frac{q^{m-2s+o(\log(m-2s))} q^{2s+o(\log s)}}{(m-2s)^+} s
\]

\[
=q^{m+o(\log m)} \sum_{s=1}^{\lfloor m/2 \rfloor} \frac{1}{s} \frac{1}{(m-2s)^+} = \frac{q^{m+o(\log m)}}{m}
\]

(66)

Note that \( q^m/m \) is an increasing function of \( m \). So if we let \( \omega = \lfloor \log n \rfloor \), then we can easily finish estimating (60):

\[
\sum_{m=1}^{n} \frac{q^m}{m} = \sum_{m=1}^{n-\omega} \frac{q^m}{m} + \sum_{m=n-\omega+1}^{n} \frac{q^m}{m}
\]

\[
\leq (n-\omega) \frac{q^{n-\omega}}{n-\omega} + \omega \frac{q^n}{n}
\]

(68)

(69)

To complete the proof of Theorem 9 all that remains is to prove that \( \sigma_1(b) = q^{k+o(\log b)} \). The sum \( \sigma_1 \) is somewhat similar to \( \sigma_2 \), and we’ll see that it can be estimated by techniques similar to those that Stong used in estimating \( \sigma_2 \). The cyclotomic polynomials satisfy a simple identity: if \( \pi_i \) is odd, then

\[
q^{\pi_i} + 1 = \frac{q^{2\pi_i} - 1}{q^{\pi_i} - 1} = \prod_{d|\pi_i} \Phi_{2d}(q).
\]

(70)

Define

- \( \Lambda = \Lambda(\pi) = \{ d : \text{for some } i, \text{ } d \text{ divides } \pi_i \} \).
- \( \nu_d(\pi) = \sum_{k \equiv 0 (d)} c_k(\pi) = \text{the number of parts that are multiples of } d, \) and
- \( w_d(\pi) = \max(0, \nu_d - 1) \).
Then
\[ \text{LCM}(q^{\pi_1} + 1, q^{\pi_2} + 1, \ldots) \leq \prod_{d \in \Lambda} \Phi_{2d} \]
\[ = \prod_{d \in \Lambda} \prod_{d \in \Lambda} (q^{\pi_i} + 1) \]  
(71)
\[ \prod_{d \in \Lambda} \Phi_{2d} \]  
(72)

If \( \pi \) is a partition of \( b \) into distinct parts, then for the numerator of (72) we have
\[ \prod_{i}(q^{\pi_i} + 1) = q^b \prod_{i}(1 - \frac{1}{q_i^{\pi_i}}) < q^b \prod_{i=1}^{\infty} \left(1 + \frac{1}{q_i^{\pi_i}}\right) < 4q^b. \]  
(73)

An upper bound is obtained if, in the denominator of (72), we restrict \( d \) to a finite set of primes. For any \( i \), let \( p_i \) denote the \( i^{th} \) prime; \( p_1 = 2, p_2 = 3, \ldots \). Given a positive integer \( \xi \), let \( \mathcal{P} = \mathcal{P}(\xi) = \{p_i : \xi \leq i \leq e^\xi\} = \{p_\xi, p_{\xi+1}, \ldots, p_{\lfloor e^\xi \rfloor}\}. \) Let \( \kappa_\xi = \prod_{p \in \mathcal{P}} \Phi_2p(q) \). Then, for any \( \pi \in \mathcal{O}_b \),
\[ \text{LCM}(q^{\pi_1} + 1, q^{\pi_2} + 1, \ldots) \leq \frac{4\kappa_\xi q^b}{\prod_{p \in \mathcal{P}} \Phi_2p}. \]  
(74)

Define
\[ G(k) = \begin{cases} \prod_{\{p, p \in \mathcal{P} \text{ and } p|k\} \Phi_2p(q)} \frac{1}{\Phi_2p(q)}, & \text{if } k \text{ is divisible by at least one prime in } \mathcal{P} \\ 1 & \text{else,} \end{cases} \]

For any partition \( \pi \), let \( z_\pi = \prod_{i=1}^{\infty} c_i^{\pi_i} \), where \( c_i = c_i(\pi) \) is the number of parts of size \( i \) that \( \pi \) has. Thus \( z_\pi = \prod_{\pi_i \geq 2} \frac{1}{\pi_i^{\pi_i-1}} \) for \( \pi \in \mathcal{O}_b \). We get an upper bound for \( \sigma_1(b) \) if we sum over all partitions of \( b \) (not just those in \( \mathcal{O}_b \)). Hence and from (71) we have
\[ \sigma_1(b) \leq 4\kappa_\xi q^b \sum_{\pi \vdash b} \frac{z_\pi}{\prod_{p \in \mathcal{P}} \Phi_2p} \]
\[ = 4\kappa_\xi q^b \sum_{\pi \vdash b} z_\pi \prod_{k=1}^{\infty} G(k)^{\frac{z_k}{k}} \]  
(75)
\[ = 4\kappa_\xi q^b \sum_{\pi \vdash b} z_\pi \prod_{k=1}^{\infty} G(k)^{\frac{z_k}{k}} \]  
(76)

In the well-known cycle index identity
\[ 1 + \sum_{b=1}^{\infty} \sum_{\pi \vdash b} z_\pi \prod_{k} x_k^{\frac{z_k}{b}} z^b = \exp \left( \sum_{k=1}^{\infty} \frac{x_k z^k}{k} \right), \]  
(77)
we can make the substitutions \( x_k = G(k), k = 1, 2, \ldots \) to get
\[ \sigma_1(b) \leq 4\kappa_\xi q^b \left[ \frac{z^b}{b} \right] \exp \left( \sum_{k=1}^{\infty} \frac{G(k) z^k}{k} \right) \]  
(78)
Following Stong, we note that the function $G(k)$ is a periodic function of $k$ with period $N = \prod_{p \in P} p$. Hence we have the Fourier expansion

$$G(k) = a_0 + \sum_{\ell=1}^{N-1} a_{\ell} e^{\omega \ell k}, \quad (79)$$

where $\omega = e^{2\pi i/N}$ and the $a_{\ell}$'s are the Fourier coefficients:

$$a_{\ell} = \frac{1}{N} \sum_{v=0}^{N-1} G(v) e^{-\ell v}. \quad (80)$$

Thus

$$\exp \left( \sum_{k=1}^{\infty} \frac{G(k)}{k} z^k \right) = \exp \left( \sum_{\ell=0}^{N-1} a_{\ell} \sum_{k=1}^{\infty} \left( e^{\ell k} z \right)^k \right) \quad (81)$$

$$= (1 - z)^{-a_0} \prod_{\ell=1}^{N-1} (1 - e^{\ell k} z)^{-a_{\ell}} \quad (82)$$

Let $\alpha = \prod_{j=1}^{N-1} (1 - \omega^j)^{-a_j}$. Because $G(k) \geq 0$ for all $k$, it is clear from $(80)$ that $|a_0| > |a_j|$ for all $j > 0$. Hence the coefficient of $z^n$ in $(81)$ and $(82)$ is asymptotic to

$$a[|z^n|] (1 - z)^{-a_0} = O \left( \frac{1}{q^{1-a_0}} \right) \quad (83)$$

It therefore suffices to verify that $a_0$ can be made arbitrarily small by choosing $\xi$ sufficiently large.

Note that, for odd primes $p$, $\Phi_{2p} = \frac{p+1}{2}$. Hence

$$G(k) \leq \begin{cases} 1 & \text{if } \gcd(k,N) = 1 \\ \frac{q+1}{q^{p\xi+1}} & \text{else} \end{cases} \quad (84)$$

Given $\epsilon > 0$, choose $\xi$ large enough so that we also have

$$\frac{q+1}{q^{p\xi+1}} < \epsilon/2. \quad (85)$$

Let $R_\xi = \{ k : \gcd(k,N) = 1 \text{ and } k \leq N \}$. By inclusion-exclusion, $|R_\xi| = \prod_{i=\xi}^{\epsilon} (1 - \frac{1}{p_i}) N$. By the prime number theorem $p_i \sim i \log i$ and consequently

$$\prod_{i=\xi}^{\epsilon} (1 - \frac{1}{p_i}) = o(1) \text{ as } \xi \to \infty. \quad \text{We can therefore also choose } \xi \text{ large enough so that } |R_\xi| \leq \frac{\epsilon}{2} N. \quad \text{But then}$$

$$a_0 = \frac{1}{N} \sum_{k=1}^{N} G(k) \leq \frac{|R_\xi|}{N} + \frac{p_\xi + 1}{q^{p\xi+1}} < \epsilon. \quad (86)$$

\[\square\]
References

[1] Elwyn R. Berlekamp, Algebraic Coding Theory, 2nd Ed., Aegean Park Press, ISBN: 0-89412-063-8

[2] Jason Fulman, Cycle indices for the finite classical groups. J. Group Theory 2 (1999), no. 3, 251–289. arXiv:math.GR/9712239

[3] Jason Fulman, Peter M. Neumann, and Cheryl E. Praeger, A generating function approach to the enumeration of matrices in classical groups over finite fields. Mem. Amer. Math. Soc. 176 (2005), no. 830.

[4] Jason Fulman, Random matrix theory over finite fields. Bull. Amer. Math. Soc. (N.S.) 39 (2002), no. 1, 51–85. arXiv:math.GR/0003195

[5] Larry C. Grove, Classical groups and geometric algebra, Graduate Studies in Mathematics 39, American Mathematical Society (2002), ISBN 0-8218-2019-2.

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

[7] R. Lidl and H. Niederreiter, Introduction to finite fields and their applications, Cambridge University Press (1994).

[8] Helmut Meyn and Werner Götz. Self-reciprocal polynomials over finite fields. Sminaire Lotharingien de Combinatoire (Oberfranken, 1990), 82–90, Publ. Inst. Rech. Math. Av., 413, Univ. Louis Pasteur, Strasbourg, 1990.

[9] Richard Stong, The average order of a matrix. J. Combin. Theory Ser. A 64 (1993), no. 2, 337–343.

[10] Richard Stong, Some asymptotic results on finite vector spaces. Adv. in Appl. Math. 9 (1988), no. 2, 167–199.

[11] Joseph L. Yucas and Gary L. Mullen, Self-Reciprocal Irreducible Polynomials Over Finite Fields, Designs, Codes, and Cryptography 33 (2004) 275–281.

[12] G.E. Wall, On the conjugacy classes in the unitary, symplectic and orthogonal groups. J. Austral. Math. Soc. 3 (1963) 1–62.