ON THE DISTRIBUTION OF THE NUMBER OF FIXED VECTORS FOR THE FINITE CLASSICAL GROUPS

JASON FULMAN AND DENNIS STANTON

Abstract. Motivated by analogous results for the symmetric group and compact Lie groups, we study the distribution of the number of fixed vectors of a random element of a finite classical group. We determine the limiting moments of these distributions, and find exactly how large the rank of the group has to be in order for the moment to stabilize to its limiting value. The proofs require a subtle use of some q-series identities. We also point out connections with orthogonal polynomials.

1. Introduction

In an influential and widely cited paper [DS], Diaconis and Shahshahani study the fixed points of random permutations, and the trace of elements of compact Lie groups. The following two theorems are special cases of their results:

Theorem 1.1. *Let π be uniformly distributed on the symmetric group S_n, and let $Z(\pi)$ denote the number of fixed points of π. Then for any natural number j, and $n \geq j$, the expected value of Z^j is equal to the Bell number B_j, the number of partitions of a set of size j. Note that B_j is the jth moment of a Poisson distribution with mean 1, so that Z approaches a Poisson distribution with mean 1 as $n \to \infty$.*

Theorem 1.2. *Let g be chosen from the Haar measure of the orthogonal group $O(n, R)$, and let $Z(g)$ denote the trace of G. Then for any natural number j, and $n \geq j$, the expected value of Z^j is equal to 0 if j is odd, and to $(j-1)(j-3)\cdots 1$ if j is even. Note that these moments are the same as the jth moment of a standard normal random variable, so that Z approaches a standard normal random variable as $n \to \infty$.*

It is natural to seek analogs of these results for the finite classical groups, and the main purpose of this paper is to provide such analogs. For example if Z denotes the number of fixed vectors of a random element of $GL(n, q)$, then for all natural numbers j and $n \geq j$, the expected value of Z^j turns out to be equal to the jth Galois number, that is the number of subspaces

Date: Submitted May 23, 2015; Revised September 8, 2015.
Key words and phrases. finite classical group, fixed space.
2010 AMS Subject Classification: 20G40, 05E15.

of a j-dimensional vector space over the finite field F_q. Moreover as $n \to \infty$, the chance that $Z = q^k$ approaches

$$\prod_{r \geq 1} \left(1 - \frac{1}{q^r}\right) \frac{1}{q^{k^2}(1-1/q)^2(1-1/q^2)^2 \cdots (1-1/q^k)^2}. \tag{1}$$

This limiting distribution can be thought of as a q-analogue of the Poisson distribution.

The starting point of our work is a beautiful, 80 page paper of Rudvalis and Shinoda [RS], which was written in 1988 and unfortunately was never published. They use Mobius inversion and a very heavy dose of combinatorics to determine, for each finite classical group G, and for each integer k, the probability that the fixed space of a random element of G is k-dimensional. For example, they show that the chance that a random element of $GL(n,q)$ has a k-dimensional fixed space is equal to:

$$\frac{1}{|GL(k,q)|} \sum_{i=0}^{n-k} \frac{(-1)^i q^{\binom{i}{2}}}{q^{ki}|GL(i,q)|}. \tag{2}$$

They also find formulae for limiting distributions such as (1).

The main purpose of the current paper is to use explicit formulas such as (2) to study the moments of the distribution of fixed vectors of random elements of finite classical groups. Looking at (2), it is not obvious that it defines a probability distribution, or how to compute its moments. We give a unified approach to such matters, for all finite classical groups (general linear, unitary, symplectic, orthogonal) in both odd and even characteristic. Other proofs of some of our results can be found in unpublished thesis work [F0] of the first named author, but the approach here is more unified and gives sharp results in all cases.

To close the introduction, we mention three reasons why our results may be of interest. First, some researchers in number theory study "Cohen-Lenstra heuristics", and need information about the distribution of fixed vectors of random elements of finite classical groups; see [W] for $GL(n,q)$ and [Ma] for the case of finite symplectic groups. Second, in the case of the symmetric groups, stability of moments of fixed points (and more generally i-cycles), has applications to representation stability in cohomology and asymptotics for families of varieties over finite fields; see Section 3.4 of [CEF] for details. We are optimistic that our results for finite classical groups might have similar applications. Third, the moment calculations of Diaconis and Shahshahani [DS] for compact Lie groups are celebrated in the random matrix community; there are various other approaches to their work [St], [PV], as well as applications of their moment calculations to studying linear functionals of eigenvalues of random matrices [DE], [J]. Rains [Ra] connects moments of traces in compact Lie groups with longest increasing subsequence problems. It is reasonable to hope that the study of moments for finite classical groups may also be fruitful.

The organization of this paper is as follows. Section 2 recalls formulae of Rudvalis and Shinoda [RS]. These explicit formulae are crucial to approach, and since their 1988 preprint never appeared, we are forced to record some of their results. In any case, we do get regular requests for a copy of the preprint [RS], so recording these formulae should be helpful to other mathematicians. Section 3 collects some q-series identities which we will use. These allow us to treat all the finite classical groups in a unified way. Section 4 contains our main results: the exact determination of how large the rank of the group has to be in order for the moments to stabilize to their limiting values (which we also determine). Section 5 uses orthogonal polynomials to give another calculation of the limiting values of the moments.

In terms of future work, it would be interesting for applications along the lines of [CEF] to prove stability results for conjugacy class functions given by fixed characters. It is natural to start with unipotent representations of $GL(n,q)$.

2. Results of Rudvalis and Shinoda

The purpose of this section is to recall some results of Rudvalis and Shinoda, dating back to 1988.

We begin with $GL(n,q)$. Recall that $|GL(n,q)| = q^{\binom{n}{2}} \prod_{i=1}^{n}(q^i - 1)$.

Theorem 2.1. (1) *The chance that an element of $GL(n,q)$ has a k-dimensional fixed space is equal to*

$$\frac{1}{|GL(k,q)|} \sum_{i=0}^{n-k} \frac{(-1)^i q^{\binom{i}{2}}}{q^{ki}|GL(i,q)|}.$$

(2) *For k fixed, the $n \to \infty$ limiting proportion of elements of $GL(n,q)$ with a k-dimensional fixed space is equal to*

$$\prod_{r \geq 1}\left(1 - \frac{1}{q^r}\right) \frac{1}{q^{k^2}\left(1-1/q\right)^2\left(1-1/q^2\right)^2 \cdots \left(1-1/q^k\right)^2}.$$

Remarks:

(1) Part 2 of Theorem 2.1 follows from part 1 of Theorem 2.1 and an identity of Euler.
(2) The proof of part 1 of Theorem 2.1 used Mobius inversion and delicate combinatorics. For a different proof, the reader can consult [F1].

Next we treat $U(n,q)$. Recall that $|U(n,q)| = q^{\binom{n}{2}} \prod_{i=1}^{n}(q^i - (-1)^i)$, and that we view $U(n,q)$ as a subgroup of $GL(n,q^2)$.

Theorem 2.2. (1) *The chance that an element of $U(n,q)$ has a k-dimensional fixed space is equal to*

$$\frac{1}{|U(k,q)|}\sum_{i=0}^{n-k}\frac{(-1)^i(-q)^{\binom{i}{2}}}{(-q)^{ki}|U(i,q)|}.$$

(2) *For k fixed, the $n \to \infty$ limiting proportion of elements of $U(n,q)$ with a k-dimensional fixed space is equal to*

$$\prod_{r\geq 0}\left(1+\frac{1}{q^{2r+1}}\right)^{-1}\frac{1}{q^{k^2}\,(1-1/q^2)\,(1-1/q^4)\cdots(1-1/q^{2k})}.$$

Remarks:

(1) Part 2 of Theorem 2.2 follows from part 1 of Theorem 2.2 and an identity of Euler.
(2) The proof of part 1 of Theorem 2.2 used Mobius inversion and delicate combinatorics. For a different proof, the reader can consult [F1].

Next we treat symplectic groups. Recall that

$$|Sp(2n,q)| = q^{n^2}\prod_{i=1}^{n}(q^{2i}-1).$$

Theorem 2.3. (1) *The proportion of elements of $Sp(2n,q)$ with a $2k$-dimensional fixed space is equal to*

$$\frac{1}{|Sp(2k,q)|}\sum_{i=0}^{n-k}\frac{(-1)^i q^{i(i+1)}}{|Sp(2i,q)|q^{2ik}}.$$

(2) *The proportion of elements of $Sp(2n,q)$ with a $2k+1$-dimensional fixed space is equal to*

$$\frac{1}{|Sp(2k,q)|q^{2k+1}}\sum_{i=0}^{n-k-1}\frac{(-1)^i q^{i(i+1)}}{|Sp(2i,q)|q^{2i(k+1)}}.$$

(3) *For k fixed, the $n \to \infty$ limiting proportion of elements of $Sp(2n,q)$ with a k-dimensional fixed space is equal to*

$$\prod_{r\geq 1}\left(1+\frac{1}{q^r}\right)^{-1}\frac{1}{q^{(k^2+k)/2}(1-1/q)(1-1/q^2)\cdots(1-1/q^k)}.$$

Remarks:

(1) Part 3 of Theorem 2.3 follows from parts 1 and 2 of Theorem 2.3 and an identity of Euler.
(2) The proof of parts 1 and 2 of Theorem 2.3 used Mobius inversion and delicate combinatorics. For a different proof, the reader can consult [F2] for the case of odd characteristic, and [FG] for the case of even characteristic.

Next we treat the orthogonal groups. Note that it is not necessary to treat odd dimensional orthogonal groups $O(2n+1,q)$ in even characteristic. Indeed, such groups are isomorphic to the symplectic groups $Sp(2n,q)$, and an element in $Sp(2n,q)$ has a k-dimensional fixed space if and only if the corresponding element in $O(2n+1,q)$ has a $k+1$-dimensional fixed space.

Theorem 2.4. *Suppose that q is odd.*

(1) *The proportion of elements of $O(2n+1,q)$ with a $2k$-dimensional fixed space is equal to*

$$\frac{1}{2}\frac{1}{q^{2k^2-k}(1-1/q^2)(1-1/q^4)\cdots(1-1/q^{2k})} \cdot\sum_{i=0}^{n-k}\frac{(-1)^i}{q^{i^2+2ik}(1-1/q^2)(1-1/q^4)\cdots(1-1/q^{2i})}.$$

(2) *The proportion of elements of $O(2n+1,q)$ with a $2k+1$-dimensional fixed space is equal to*

$$\frac{1}{2}\frac{1}{q^{2k^2+k}(1-1/q^2)(1-1/q^4)\cdots(1-1/q^{2k})} \cdot\sum_{i=0}^{n-k}\frac{(-1)^i}{q^{i^2+2i(k+1)}(1-1/q^2)(1-1/q^4)\cdots(1-1/q^{2i})}.$$

(3) *For k fixed, the $n\to\infty$ limiting proportion of elements of $O(2n+1,q)$ with a k-dimensional fixed space is equal to*

$$\prod_{r\geq 0}\left(1+\frac{1}{q^r}\right)^{-1}\frac{1}{q^{(k^2-k)/2}(1-1/q)(1-1/q^2)\cdots(1-1/q^k)}.$$

Remarks:

(1) Part 3 of Theorem 2.4 follows from parts 1 and 2 of Theorem 2.4 and an identity of Euler.
(2) The proof of parts 1 and 2 of Theorem 2.4 used Mobius inversion and delicate combinatorics. For a different proof, the reader can consult [F2].

Finally, we consider even dimensional orthogonal groups. Note that the formulas are the same in odd and even characteristic.

Theorem 2.5. (1) *The proportion of elements of $O^{\pm}(2n,q)$ with a $2k$-dimensional fixed space is equal to*

$$\frac{q^k}{2|GL(k,q^2)|}\sum_{i=0}^{n-k}\frac{(-1)^i}{q^{(2k-1)i}(q^{2i}-1)\cdots(q^4-1)(q^2-1)} \pm\frac{1}{2}\frac{(-1)^{n-k}}{q^{2k(n-k)}|GL(k,q^2)|(q^{2(n-k)}-1)\cdots(q^4-1)(q^2-1)}.$$

(2) *The proportion of elements of* $O^{\pm}(2n,q)$ *with a* $2k+1$*-dimensional fixed space is*

$$\frac{1}{2q^k|GL(k,q^2)|}\sum_{i=0}^{n-k-1}\frac{(-1)^i}{q^{i^2+2(k+1)i}(1-1/q^2)(1-1/q^4)\cdots(1-1/q^{2i})}.$$

(3) *For* k *fixed, the* $n\to\infty$ *limiting proportion of elements of* $O^{\pm}(2n,q)$ *with a* k*-dimensional fixed space is equal to*

$$\prod_{r\geq 0}\left(1+\frac{1}{q^r}\right)^{-1}\frac{1}{q^{(k^2-k)/2}(1-1/q)(1-1/q^2)\cdots(1-1/q^k)}.$$

Remarks:

(1) Note that for Theorem 2.5, the third part follows from parts 1 and 2, and an identity of Euler.
(2) The proof of parts 1 and 2 of Theorems 2.5 used Mobius inversion and delicate combinatorics. For a different proof, the reader can consult [F2] for the case of odd characteristic, and [FST] for the case of even characteristic.

3. q-SERIES IDENTITIES

The purpose of this section is to collect the q-series identities which will be used in the proofs of our main theorems.

We use the standard notation [GaRa, (I.1),(I.42)] for the q-shifted factorial and the q-binomial coefficient

$$(A;q)_n=(1-A)(1-Aq)\cdots(1-Aq^{n-1}),$$
$$\binom{n}{k}_q=\frac{(q^n-1)\cdots(q^{n-k+1}-1)}{(q^k-1)\cdots(q-1)}=\frac{(q^n;q^{-1})_k}{(q;q)_k}.$$

Note that all of the numerical quantities in Section 2 can be written in terms of q-shifted factorials.

Proposition 3.1. *We have*

$$|GL(n,q)|=(q^n-1)\cdots(q^n-q^{n-1})=(-1)^nq^{\binom{n}{2}}(q;q)_n,$$
$$|U(n,q)|=q^{\binom{n}{2}}\prod_{i=1}^{n}(q^i-(-1)^i)=Q^{\binom{n}{2}}(Q;Q)_n,\quad Q=-q,$$
$$|Sp(2n,q)|=q^{n^2}(q^2-1)\cdots(q^{2n}-1)=(-1)^nR^{n^2/2}(R;R)_n,\quad R=q^2.$$

A certain double sum occurs in each of our results; we next define a general such sum.

Definition 3.2. *Let*

$$D_n(P,X,Y)=\sum_{k=0}^{n}\frac{(-X)^k}{P^{\binom{k}{2}}(P;P)_k}\sum_{i=0}^{n-k}\frac{P^{-ik}Y^i}{(P;P)_i}.$$

Proposition 3.3. *If j is a non-negative integer,*

$$D_n(P, YP^j, Y) = \sum_{J=0}^{n} \binom{j}{J}_P Y^J.$$

Proof. Let $J = k + i$. The double sum $D_n(P, X, Y)$ can be rewritten as

$$\begin{aligned} D_n(P, X, Y) &= \sum_{J=0}^{n} \sum_{k=0}^{J} \frac{(-X)^k Y^{J-k} P^{-\binom{k}{2}} P^{-k(J-k)}}{(P;P)_{J-k}(P;P)_k} \\ &= \sum_{J=0}^{n} \frac{Y^J}{(P;P)_J} \sum_{k=0}^{J} \binom{J}{k}_P P^{\binom{k}{2}} (-1)^k (XP^{1-J}/Y)^k. \end{aligned}$$

Now use the q-binomial theorem (page 78 of [Br])

$$\sum_{k=0}^{J} \binom{J}{k}_P P^{\binom{k}{2}} (-1)^k Z^k = (Z;P)_J \tag{3}$$

with $Z = XP^{1-J}/Y$ to evaluate the inner sum as $(XP^{1-J}/Y;P)_J$. So

$$D_n(P, X, Y) = \sum_{J=0}^{n} \frac{(XP^{1-J}/Y;P)_J}{(P;P)_J} Y^J \tag{4}$$

If $X = YP^j$, then

$$\frac{(XP^{1-J}/Y;P)_J}{(P;P)_J} = \binom{j}{J}_P$$

□

One may use Proposition 3.3 with $j = -1$ (namely (4) with $X = YP^{-1}$) to obtain the next result.

Proposition 3.4. *If n is a non-negative integer,*

$$D_n(P, YP^{-1}, Y) = \sum_{J=0}^{n} P^{-\binom{J+1}{2}} (-Y)^J.$$

Next, because the sum in Proposition 3.3 later occurs with special choices of Y, we record three simple evaluations. The first identity ([A, p. 37]) occurs for the unitary groups, while the last two ([A, p. 49]) will be helpful in treating the symplectic and orthogonal groups.

Proposition 3.5. (1) *For any non-negative integer j,*

$$\sum_{J=0}^{2j} \binom{2j}{J}_q (-1)^J = (q;q^2)_j.$$

(2) *For any non-negative integer n,*

$$\sum_{J=0}^{n} \binom{n}{J}_q q^{J/2} = (-q^{1/2};q^{1/2})_n.$$

(3) *For any non-negative integer* n,

$$\sum_{J=0}^{n} \binom{n}{J}_q q^{-J/2} = (-q^{1/2}; q^{1/2})_n / q^{n/2}.$$

Finally we record a generating function related to the double sum.

Proposition 3.6. *If* $0 < a < 1$, $|P| > 1$, *and*

$$D_{nk} = \frac{(-X)^k}{P^{\binom{k}{2}}(P;P)_k} \sum_{i=0}^{n-k} \frac{P^{-ik} Y^i}{(P;P)_i},$$

then

$$\begin{aligned} F_k(a, X, Y; P) :=& (1-a) \sum_{n=k}^{\infty} D_{nk} a^n \\ =& (aYP^{-1}; P^{-1})_\infty \frac{(aX)^k P^{-k^2}}{(P^{-1}; P^{-1})_k (aYP^{-1}; P^{-1})_k}. \end{aligned}$$

Proof. In the double sum definition of $F_k(a, X, Y; P)$, replace n by $n + k + i$ to obtain

$$\begin{aligned} F_k(a, X, Y; P) =& (1-a) \sum_{0 \le n, i} a^{n+i} \frac{(-aX)^k}{P^{\binom{k}{2}}(P;P)_k} \frac{P^{-ik} Y^i}{(P;P)_i} \\ =& \frac{(aX)^k P^{-k^2}}{(P^{-1}; P^{-1})_k} \sum_{i=0}^{\infty} \frac{P^{-\binom{i}{2}} (-YP^{-1-k})^i}{(P^{-1}; P^{-1})_i} a^i. \end{aligned}$$

Applying a limiting case of the q-binomial theorem

$$\begin{aligned} \sum_{i=0}^{\infty} \frac{P^{-\binom{i}{2}}}{(P^{-1}; P^{-1})_i} (-P^{-1-k} Ya)^i =& (aYP^{-1-k}; P^{-1})_\infty \\ =& \frac{(aYP^{-1}; P^{-1})_\infty}{(aYP^{-1}; P^{-1})_k} \end{aligned}$$

completes the proof. □

Remark 3.7. *If* $X = Y$, *then* $F_k(a, X, Y; P)$ *may be summed by a limiting case of the q-Gauss sum,* [GaRa, (II.8)],

$$\sum_{k=0}^{\infty} F_k(a, X, X; P) = 1.$$

This is the probability measure in Proposition 5.1.

4. Main results

This section proves our main results about the distribution of the number of fixed vectors of a random element of a finite classical group. We determine the limiting moments of these distributions, and find precisely how large the rank of the group has to be in order for the moment to stabilize to its limiting value.

Theorem 4.1 treats the general linear groups.

Theorem 4.1. *Let the random variable Z_n be the number of fixed vectors of a random element of $GL(n,q)$ in its natural action. Then for all natural numbers j, and $n \geq j$, the expected value of Z_n^j is equal to the number of subspaces of a j-dimensional vector space over the finite field F_q.*

Proof. Part 1 of Theorem 2.1 implies that

$$\begin{aligned} E[Z_n^j] &= \sum_{k=0}^{n} P(Z_n = q^k) q^{jk} \\ &= \sum_{k=0}^{n} \frac{q^{jk}}{|GL(k,q)|} \sum_{i=0}^{n-k} \frac{(-1)^i q^{\binom{i}{2}}}{q^{ki}|GL(i,q)|} = D_n(q, q^j, 1), \end{aligned}$$

where D_n is given by Definition 3.2.

Proposition 3.3 implies

$$D_n(q, q^j, 1) = \sum_{J=0}^{n} \binom{j}{J}_q = \sum_{J=0}^{min(n,j)} \binom{j}{J}_q.$$

For $n \geq j$, this is the number of subspaces of a j-dimensional vector space over the finite field F_q. □

Remark 4.2. *The proof of Theorem 4.1 shows that if $n < j$, then the jth moment has not stabilized to its limiting value.*

Remark 4.3. *The number of subspaces of a j-dimensional vector space over the finite field F_q has been studied by Goldman and Rota* [GR]*, who named these numbers the Galois numbers G_j. They proved the recurrence*

$$G_{j+1} = 2G_j + (q^j - 1)G_{j-1}.$$

Another proof of Theorem 4.1 is in unpublished thesis work [F0] of the first named author, and goes as follows.

Proof. Let $G = GL(n,q)$ and let X be the product of j copies of V, where V is the n-dimensional vector space on which G acts. Let G act on X by acting separately on each coordinate.

Consider the average number of fixed points of G on X. On one hand, this is the jth moment of the distribution of fixed vectors of G on V. On the other hand, by Burnside's lemma this is the number of orbits of G on X. To each orbit of G on X, define an invariant k of the orbit (called the

number of parts of the orbit) by taking any element $(v_1, \cdots, v_j)$ in the orbit and letting k be the dimension of the span of $v_1, \cdots, v_j$.

We claim that for $n \geq j$, the total number of orbits with invariant k is equal to the q-binomial coefficient $\binom{j}{k}_q$, the number of k-dimensional subspaces of a j-dimensional vector space. This is proved bijectively. Given an orbit, let $i_1, \cdots, i_k$ be the positions i such that the dimension of the span of $v_1, \cdots, v_i$ is one more than the dimension of the span of $v_1, \cdots, v_{i-1}$. Let $(v_1, \cdots, v_j)$ be the unique element of the orbit such that $v_{i_1}, \cdots, v_{i_k}$ are the standard basis vectors $e_1, \cdots, e_k$. Let M be the $n \times j$ matrix whose columns are the vectors $v_1, \cdots, v_j$. Let M' be M with the last $n-k$ rows chopped off, so that M' is a $k \times j$ matrix. Note that M' is in reduced row-echelon form, and hence by basic linear algebra corresponds to a unique k-dimensional subspace of a j-dimensional space. □

Next we treat the unitary groups $U(n,q)$. Since $U(n,q)$ is viewed as a subgroup of $GL(n,q^2)$, an element of $U(n,q)$ with a k-dimensional fixed space has q^{2k} many fixed vectors.

Theorem 4.4. *Let the random variable Z_n be the number of fixed vectors of a random element of $U(n,q)$ in its natural action. Then for all natural numbers j, and $n \geq 2j$, the expected value of Z_n^j is equal to*

$$\prod_{i=1}^{j}(q^{2i-1}+1).$$

Proof. Let $Q = -q$. Theorem 2.2(1) yields

$$E[Z_n^j] = \sum_{k=0}^{n} \frac{q^{2jk}}{|U(k,q)|} \sum_{i=0}^{n-k} \frac{(-1)^i (-q)^{\binom{i}{2}}}{(-q)^{ki}|U(i,q)|} = D_n(Q, -Q^{2j}, -1).$$

By Proposition 3.3 and Proposition 3.5(1) we have

$$\begin{aligned} D_n(Q, -Q^{2j}, -1) &= \sum_{J=0}^{n} \binom{2j}{J}_Q (-1)^J \\ &= (Q;Q^2)_j = \prod_{i=1}^{j}(q^{2i-1}+1) \text{ if } n \geq 2j. \end{aligned}$$

□

Remark 4.5. *To see that the bound in Theorem 4.4 is sharp, note that when $n = j = 1$, $E[Z_1^1]$ is equal to q.*

Next we treat the symplectic groups.

Theorem 4.6. *Let the random variable Z_n be the number of fixed vectors of a random element of $Sp(2n,q)$ in its natural action. Then for all natural*

numbers j, and $n \geq j$, the expected value of Z_n^j is equal to

$$\prod_{i=1}^{j}(q^{i-1}+1).$$

Proof. We treat the cases $j = 0$ and $j > 0$ separately.

Suppose first that $j = 0$. From parts 1 and 2 of Theorem 2.3, there are two double sums to consider, and let $R = q^2$. The first double sum is

$$\sum_{k=0}^{n} \frac{1}{|Sp(2k,q)|} \sum_{i=0}^{n-k} \frac{(-1)^i q^{i(i+1)}}{|Sp(2i,q)|q^{2ik}} = D_n(R, q^{-1}, q) = \sum_{J=0}^{n}(-1)^J q^{-J^2}$$

where we have used Proposition 3.4.

The second double sum is

$$\sum_{k=0}^{n-1} \frac{1}{q^{2k+1}|Sp(2k,q)|} \sum_{i=0}^{n-k-1} \frac{(-1)^i q^{i(i+1)}}{q^{2i(k+1)}|Sp(2i,q)|} = \frac{1}{q} D_{n-1}(R, q^{-3}, q^{-1}).$$

which by Proposition 3.4 is

$$\sum_{J=0}^{n-1}(-1)^J q^{-(J+1)^2}.$$

The $j = 0$ case of the theorem now follows since

$$\sum_{J=0}^{n}(-1)^J q^{-J^2} + \sum_{J=0}^{n-1}(-1)^J q^{-(J+1)^2} = 1.$$

Next we consider the case that $j \geq 1$. Again by parts 1 and 2 of Theorem 2.3, there are two double sums. The first double sum is

$$\sum_{k=0}^{n} \frac{q^{2kj}}{|Sp(2k,q)|} \sum_{i=0}^{n-k} \frac{(-1)^i q^{i(i+1)}}{|Sp(2i,q)|q^{2ik}} = D_n(R, q^{2j-1}, q) = \sum_{J=0}^{n} \binom{j-1}{J}_R R^{\frac{J}{2}}.$$

By Proposition 3.5(2), this is equal to $(-q;q)_{j-1}$ if $n \geq j-1$.

Again using Proposition 3.3 and Proposition 3.5(3), the second double sum is

$$\begin{aligned}
&\sum_{k=0}^{n-1} \frac{q^{(2k+1)j}}{|Sp(2k,q)|q^{2k+1}} \sum_{i=0}^{n-k-1} \frac{(-1)^i q^{i(i+1)}}{q^{2i(k+1)}} \frac{1}{|Sp(2i,q)|} \\
&= q^{j-1} D_{n-1}(R, q^{2j-3}, q^{-1}) = q^{j-1} \sum_{J=0}^{n-1} \binom{j-1}{J}_R R^{-J/2} \\
&= (-q;q)_{j-1} \text{ if } n \geq j.
\end{aligned}$$

The theorem now follows since if $n \geq j$,

$$E[Z_n^j] = 2(-q;q)_{j-1} = 2(1+q)\cdots(1+q^{j-1}) = \prod_{i=1}^{j}(q^{i-1}+1).$$

□

Remark 4.7. *The $j = 0$ case of Theorem 4.6 is trivially true since any probability distribution sums to 1. However we feel that the proof of this case in the proof of Theorem 4.6 is of interest.*

Remark 4.8. *To see that the bound in Theorem 4.6 is sharp, note that when $j = 2$ and $n = 1$, $E[Z_1^2]$ is equal to $2q + 1$.*

Next we treat the odd characteristic, odd dimensional orthogonal groups $O(2n+1, q)$. As explained just before the proof of Theorem 2.4, there is no need to treat odd dimensional orthogonal groups in even characteristic.

Theorem 4.9. *Suppose that the characteristic is odd. Let the random variable Z_n be the number of fixed vectors of a random element of $O(2n+1, q)$ in its natural action. Then for all natural numbers j, and $n \geq j$, the expected value of Z_n^j is equal to*

$$\prod_{i=1}^{j}(q^i + 1).$$

Proof. The proof is nearly the same as that of Theorem 4.6, so we abbreviate the details. From parts 1 and 2 of Theorem 2.4, there are two double sums, and we let $R = q^2$. The first double sum is

$$\frac{1}{2}D_n(R, q^{2j+1}, q) = \frac{1}{2}\sum_{J=0}^{n}\binom{j}{J}_R R^{J/2}.$$

If $n \geq j$, then this is equal to $\frac{1}{2}(-q; q)_j$ by Proposition 3.5(2).

The second double sum is

$$\frac{1}{2}q^j D_n(R, q^{2j-1}, 1/q) = \frac{1}{2}q^j \sum_{J=0}^{n}\binom{j}{J}_R R^{-J/2}.$$

If $n \geq j$, then this is equal to $\frac{1}{2}(-q; q)_j$ by Proposition 3.5(3).

So the two double sums are equal, and adding their values gives the required $(-q; q)_j = \prod_{i=1}^{j}(q^i + 1)$. □

Remark 4.10. *To see that the bound in Theorem 4.9 is sharp, note that when $j = 1$ and $n = 0$, $E[Z_0^1]$ is equal to $(q + 1)/2$.*

Next we consider even dimensional orthogonal groups. As mentioned in Section 2, the formulas are the same in even and odd characteristic. We first treat $O^+(2n, q)$, and then treat $O^-(2n, q)$. Note that the moments stabilize more quickly for $O^+(2n, q)$ than for $O^-(2n, q)$.

Theorem 4.11. *Let the random variable Z_n be the number of fixed vectors of a random element of $O^+(2n, q)$ in its natural action. Then for all natural numbers j, and $n \geq j$, the expected value of Z_n^j is equal to*

$$\prod_{i=1}^{j}(q^i + 1).$$

Proof. From parts 1 and 2 of Theorem 2.5, there are two double sums and a single sum, and we let $R = q^2$.

The first double sum is:

$$\frac{1}{2} D_n(R, q^{2j+1}, q),$$

which is equal to $\frac{1}{2}(-q;q)_j$ if $n \geq j$.

Next, for the single sum one computes that

$$\begin{aligned} & \frac{1}{2} \sum_{k=0}^{n} \frac{(-1)^{n-k} q^{2kj}}{q^{2k(n-k)} |GL(k, q^2)| (q^{2(n-k)} - 1) \cdots (q^2 - 1)} \\ = \; & \frac{1}{2} \frac{1}{(R;R)_n} \sum_{k=0}^{n} \binom{n}{k}_R (-1)^k R^{\binom{k}{2}} (R^{j+1-n})^k \\ = \; & \frac{1}{2} \frac{1}{(R;R)_n} (R^{j+1-n}; R)_n, \end{aligned}$$

where the last step used the q-binomial theorem (3). Note that

$$\frac{1}{2} \frac{1}{(R;R)_n} (R^{j+1-n}; R)_n$$

is equal to $\frac{1}{2}$ if $n = j$, and to 0 if $n > j$. Summarizing, the even dimensional fixed spaces contribute

$$\begin{cases} \frac{1}{2}\left[(-q;q)_j + 1\right] & \text{if } n = j \\ \frac{1}{2}\left[(-q;q)_j\right] & \text{if } n > j \end{cases}$$

Next consider the contribution from the odd dimensional fixed spaces in Theorem 2.5. It is

$$\frac{q^j}{2} D_{n-1}(R, q^{2j-1}, q^{-1}) = \frac{q^j}{2} \sum_{J=0}^{n-1} \binom{j}{J}_R R^{-J/2}.$$

By Proposition 3.5(3), this is equal to $\frac{1}{2}(-q;q)_j$ if $n > j$, and to $\frac{1}{2}[(-q;q)_j - 1]$ if $n = j$. Summarizing, this contribution is

$$\begin{cases} \frac{1}{2}\left[(-q;q)_j - 1\right] & \text{if } n = j \\ \frac{1}{2}\left[(-q;q)_j\right] & \text{if } n > j \end{cases}$$

Adding the values of the two contributions completes the proof. □

Remark 4.12. *To see that the bound in Theorem 4.11 is sharp, note that when $j = 2$ and $n = 1$, $E[Z_1^2] = (q^2 + 1)(q + 2)/2$.*

Theorem 4.13. *Let the random variable Z_n be the number of fixed vectors of a random element of $O^-(2n, q)$ in its natural action. Then for all natural numbers j, and $n \geq j + 1$, the expected value of Z_n^j is equal to*

$$\prod_{i=1}^{j} (q^i + 1).$$

Proof. The proof is very similar to that of Theorem 4.11. □

Remark 4.14. *To see that the bound in Theorem 4.13 is sharp, note that when* $n = j = 1$, $E[Z_1^1] = q$.

5. Connections to classical orthogonal polynomials

The limiting distribution in Theorem 2.1(2) is a q-analogue of the Poisson distribution. It may be identified as a special case of the distribution for Al-Salam-Carlitz polynomials. For the limiting cases of the other classical groups, Theorems 2.2(2), 2.3(3), 2.4(3), 2.5(3) there is another q-analogue of the Poisson distribution which plays this role- the distribution for the q-Charlier polynomials. In this section we recall the definition of these classical polynomials and note that their known moments agree with our main results.

The analogous question for the symmetric group is answered by the Charlier polynomials $C_n(x; a)$ with $a = 1$ (see Theorem 1.1). These polynomials are orthogonal with respect to the Poisson distribution

$$w_{Char}(k, a) = e^{-a}\frac{a^k}{k!}, \quad k = 0, 1, \cdots .$$

Our two q-versions are also discrete distributions. First we recall the Al-Salam-Carlitz polynomials, see [Ch, p. 195-198], [C, p. 23-24].

Proposition 5.1. *Let* $0 < p < 1$ *and* $a > 0$. *The Al-Salam-Carlitz polynomials* $V_n^{(a)}(x; p)$ *are orthogonal with respect to the discrete probability measure which is supported on the sequence* p^{-k} *with masses of*

$$w_{AC}(p^{-k}; a; p) \;=\; (ap; p)_\infty \frac{p^{k^2} a^k}{(p; p)_k (ap; p)_k}, \quad k = 0, 1, \cdots , .$$

Remark 5.2. *Note the following limiting case of the Al-Salam-Carlitz weight to the Poisson distribution*

$$\lim_{p \to 1} w_{AC}(p^{-k}, (1 - p)a; p) = e^{-a}\frac{a^k}{k!}.$$

Theorem 5.3. *The limiting measure in Theorem 2.1(2) is given by the choice of* $p = 1/q$ *and* $a = 1$ *in the Al-Salam-Carlitz polynomials in Proposition 5.1.*

For the other limiting cases we use a classical q-Charlier polynomial [GaRa, Exer. 7.13, p. 202], whose measure is also purely discrete.

Proposition 5.4. *Let* $0 < p < 1$ *and* $a > 0$. *The p-Charlier polynomials* $C_n(x; a, p)$ *are orthogonal with respect to the discrete probability measure which is supported on the sequence* p^{-k} *with masses of*

$$w_{p-Char}(p^{-k}; a, p) \;=\; \frac{1}{(-a; p)_\infty} \frac{p^{\binom{k}{2}}}{(p; p)_k} a^k, \quad k = 0, 1, \cdots , .$$

Remark 5.5. *Note the following limiting case of the q-Charlier weight to the Poisson distribution*

$$\lim_{p\to 1} w_{p-Char}(p^{-k},(1-p)a;p) = e^{-a}\frac{a^k}{k!}.$$

Theorem 5.6. *The remaining limiting cases of the distributions are*

1. *Theorem 2.2(2) corresponding to p-Charlier polynomials with* $p = 1/q^2$, $a = 1/q$,
2. *Theorem 2.3(3) corresponding to p-Charlier polynomials with* $p = 1/q$, $a = 1/q$,
3. *Theorem 2.4(3) corresponding to p-Charlier polynomials with* $p = 1/q$, $a = 1$,
4. *Theorem 2.5(3) corresponding to p-Charlier polynomials with* $p = 1/q$, $a = 1$.

Our main theorems give stabilizing values of the moments. For permutations, Theorem 1.1 gives Bell numbers as these stabilizing moments. The moments for the Charlier polynomial distribution are known to be

$$\mu_j^{Char} = \sum_{k=1}^{j} S(j,k)a^k, \tag{5}$$

where $S(j,k)$ are Stirling numbers of the second kind. The Stirling numbers refine the Bell numbers

$$B_j = \sum_{k=1}^{j} S(j,k),$$

so these are the moments for the Poisson distribution with mean $a = 1$.

We have the following known results for the moments of our two q-Poisson distributions.

Proposition 5.7.

The moments μ_j^{AC} *for the distribution of Al-Salam-Carlitz polynomials are given by* [Ch, (10.10)]

$$\mu_j^{AC} = \sum_{k=0}^{j} \binom{j}{k}_{1/p} a^k.$$

The moments μ_j^{q-Char} *for the distribution of q-Charlier polynomials are given by* [DSW, §7]

$$\mu_j^{q-Char} = (-a/p;1/p)_j.$$

We see that in all cases, Theorems 4.1, 4.4, 4.6, 4.9, 4.11, 4.13, the stabilizing value of the moment is equal to the moment of the limiting distribution.

The moments given in Proposition 5.7 do not appear to be a natural q-analogue of (5). One would expect to see a q-analogue of Stirling numbers of the second kind. This may be accomplished by applying an affine change

of variable, so that the support of the measure has the limiting value k when $q \to 1$.

Proposition 5.8. *If the Al-Salam-Carlitz polynomials are rescaled so that the measure is located at $(q^{-k}-1)/(1-q)$, which has a limiting value of k as $q \to 1$, and a is replaced by $(1-q)a$, the moments are given by q-Stirling numbers (see* [DSW, (3.2)]*)*

$$\mu_j^{AC} = q^{-j} \sum_{k=1}^{j} q^k S_{1/q}(j,k) a^k.$$

If the q-Charlier polynomials are rescaled so that the measure is located at $(q^{-k}-1)/(1-q)$, which has a limiting value of k as $q \to 1$, and a is replaced by $(1-q)a$, the moments are given by q-Stirling numbers [DSW, (7.4)]

$$\mu_j^{q-Char} = q^{-j} \sum_{k=1}^{j} q^{-\binom{k}{2}} S_{1/q}(j,k) a^k.$$

The Poisson distribution is a determinate Hamburger moment problem. In our q-Charlier distributions, one may ask if the limiting distributions we gave are guaranteed once the moments are given. However the answer is no, both problems are indeterminate, [C, p. 23-24].

As the moment matching suggests (and as one can prove using the explicit formulae in Section 2), convergence to the limiting distributions (in total variation distance) is extremely rapid.

For example, in the case of the general linear groups, one has the following result. Recall that the total variation distance between two probability measures P, Q on a set X is defined as $\frac{1}{2}\sum_{x \in X} |P(x) - Q(x)|$.

Theorem 5.9. *Let $P_{GL,n}$ be the probability measure on the natural numbers whose value at k is equal to the probability that a random element of $GL(n,q)$ has a k-dimensional fixed space. Let $P_{GL,\infty}$ be the probability measure on the natural numbers given by part 2 of Theorem 2.1. Then the total variation distance between $P_{GL,n}$ and $P_{GL,\infty}$ is at most $C/q^{(n^2+3n)/2+1}$, for a universal constant C.*

Proof. Suppose that $0 \leq k \leq n$. By part 1 of Theorem 2.1, $P_{GL,n}(k)$ is a sum of terms which alternate in sign and decrease in magnitude. Thus

$$\begin{aligned} |P_{GL,n}(k) - P_{GL,\infty}(k)| &\leq \frac{1}{|GL(k,q)|} \frac{q^{\binom{n-k+1}{2}}}{q^{k(n-k+1)}|GL(n-k+1,q)|} \\ &\leq \frac{Aq^{\binom{n-k+1}{2}}}{q^{k^2} q^{k(n-k+1)} q^{(n-k+1)^2}} \\ &= \frac{A}{q^{n^2/2+3n/2+1+k^2/2-k/2}}, \end{aligned}$$

for a universal constant A. Thus

$$\sum_{k=0}^{n} |P_{GL,n}(k) - P_{GL,\infty}(k)| \leq \frac{B}{q^{n^2/2+3n/2+1}}$$

for a universal constant B.

For $k > n$, $P_{GL,n}(k) = 0$ and $P_{GL,\infty}(k) \leq A/q^{k^2}$ for a universal constant A. Thus

$$\sum_{k=n+1}^{\infty} |P_{GL,n}(k) - P_{GL,\infty}(k)| \leq \frac{B}{q^{(n+1)^2}}$$

for a universal constant B. The result follows. □

All values of n may be considered simultaneously by choosing a random n. We use the fact that the Al-Salam-Carlitz weight satisfies

$$F_k(a, X, X; P) = w_{AC}(p^{-k}; aX; p), \quad P = 1/p.$$

First we consider $GL(n, q)$.

Theorem 5.10. *Suppose that a non-negative integer n is chosen with probability $(1-a)a^n$. Then the probability that a random element of a random $GL(n, q)$ has q^k fixed vectors is given by the probability measure in Proposition 5.1 with $p = 1/q$.*

Proof. We need

$$\sum_{n=0}^{\infty} P(Z_n = q^k)a^n(1-a) = F_k(a, 1, 1; q) = w_{AC}(p^{-k}; a; p), \quad p = 1/q.$$

This result also appears in [F1]. □

For the unitary groups, note that the proof of Theorem 4.4 used the values $D_n(Q, -Q^{2j}, -1)$, $Q = -q$. So we need

$$\begin{aligned}\sum_{n=0}^{\infty} P(Z_n = q^{2k})a^n(1-a) &= F_k(a, -1, -1; Q) \\ &= w_{AC}(p^{-k}; -a; p), \quad p = 1/Q = -1/q.\end{aligned}$$

Theorem 5.11. *Suppose that a non-negative integer n is chosen with probability $(1-a)a^n$. Then the probability that a random element of a random $U(n, q)$ has q^{2k} fixed vectors is given by the probability measure in Proposition 5.1 with $p = -1/q$ and a replaced by $-a$.*

For the symplectic groups, there are two cases in Theorem 2.3, depending upon the fixed point space being even or odd dimensional. Curiously, these two cases may be combined into a single example of the Al-Salam-Carlitz weight. This is analogous to the association scheme of symmetric matrices, where adjacent ranks are combined depending on the parity, see [Eg].

Theorem 5.12. *Suppose that a non-negative integer n is chosen with probability $(1-a)a^n$. Then the probability that a random element of a random $Sp(2n,q)$ has q^{2k} or q^{2k+1} fixed vectors is given by the probability measure in Proposition 5.1 with $p = 1/q^2$ and a replaced by a/q.*

Proof. The proof of Theorem 4.6 used two terms for $j = 0$,

$$D_n(R, q^{-1}, q) + \frac{1}{q} D_{n-1}(R, q^{-3}, q^{-1}).$$

So we need for $P = R = q^2$,

$$\begin{aligned}
&\sum_{n=0}^{\infty} \left(P(Z_n = q^{2k}) + P(Z_n = q^{2k+1}) \right) a^n (1-a) \\
&\quad = F_k(a, q^{-1}, q; P) + \frac{a}{q} F_k(a, q^{-3}, q^{-1}; P) \\
&\quad = (aq^{-1}P^{-1}; P^{-1})_\infty \frac{(aq^{-1})^k P^{-k^2}}{(P^{-1}; P^{-1})_k (aq^{-1}P^{-1}; P^{-1})_k} \\
&\quad = w_{AC}(P^k; aq^{-1}; P^{-1}).
\end{aligned}$$

□

6. Acknowledgements

Fulman was partially supported by NSA grant H98230-13-1-0219. Stanton was partially supported by NSF grant DMS-1148634. The authors thank Persi Diaconis and a referee for helpful remarks.

References

[A] Andrews, G., The theory of partitions, Addison-Wesley, Reading, Mass., 1976.

[Br] Bressoud, D., Proofs and confirmations. The story of the alternating sign matrix conjecture, Cambridge University Press, Cambridge, 1999.

[Ch] Chihara, T., An Introduction to Orthogonal Polynomials, Gordon and Breach Science Publishers, New York-London-Paris, 1978.

[C] Christiansen, J., Indeterminate moment problems within the Askey-scheme, Ph. D. thesis, University of Copenhagen, 2004.

[CEF] Church, T., Ellenberg, J., and Farb, B., Representation stability in cohomology and asymptotics for families of varieties over finite fields, in *Contemporary Mathematics* **620** (2014), 1-54.

[DSW] de Medicis, A., Stanton, D., and White, D., The combinatorics of q-Charlier polynomials, *J. Combin. Th. Ser. A* **69** (1995), 87-114.

[DE] Diaconis, P. and Evans, S., Linear functionals of eigenvalues of random matrices, *Trans. Amer. Math. Soc.* **353** (2001), 2615-2633.

[DS] Diaconis, P. and Shahshahani, M., On the eigenvalues of random matrices, *J. Appl. Probab.* **31A** (1994), 49-62.

[Eg] Egawa, Y., Association schemes of quadratic forms, *J. Combin. Th. Ser. A* **38** (1985), 1-14.

[F0] Fulman, J., Probability in the classical groups over finite fields, Ph.D. thesis, Harvard University, 1997.

[F1] Fulman, J., A probabilistic approach toward conjugacy classes in the finite general linear and unitary groups, *J. Algebra* **212** (1999), 557-590.

[F2] Fulman, J., A probabilistic approach to conjugacy classes in the finite symplectic and orthogonal groups, *J. Algebra* **234** (2000), 207-224.

[FG] Fulman, J. and Guralnick, R., Conjugacy class properties of the extension of $GL(n,q)$ generated by the inverse transpose involution, *J. Algebra* **275** (2004), 356-396.

[FST] Fulman, J., Saxl, J., and Tiep, P.H., Cycle indices for finite orthogonal groups of even characteristic, *Trans. Amer. Math. Soc.* **364** (2012), 2539-2566.

[GaRa] Gasper, G., and Rahman, M., Basic Hypergeometric Series, Second edition. Encyclopedia of Mathematics and its Applications, 96. Cambridge University Press, Cambridge, 2004.

[GR] Goldman, J. and Rota, G.-C., The number of subspaces of a vector space, in *Recent Progress in Combinatorics (Proc. Third Waterloo Conf. on Combinatorics).* (1969), 75-83.

[J] Johansson, K., On random matrices from the compact Lie groups, *Ann. of Math.* **145** (1997), 519-545.

[Ma] Malle, G., On the distribution of class groups of number fields, *Experiment. Math.* **19** (2010), 465-474.

[PV] Pastur, L. and Vasilchuk, V., On the moments of traces of matrices of classical groups, *Comm. Math. Phys.* **252** (2004), 149-166.

[Ra] Rains, E., Increasing subsequences and the classical groups, *Electron. J. Combin.* **5** (1998), Research Paper 12, 9 pp. (electronic).

[RS] Rudvalis, A. and Shinoda, K., An enumeration in finite classical groups. U-Mass Amherst Department of Mathematics Technical Report, 1988.

[St] Stolz, M., On the Diaconis-Shahshahani method in random matrix theory, *J. Algebraic Combin.* **22** (2005), 471-491.

[W] Washington, L., Some remarks on Cohen-Lenstra heuristics, *Math. Comp.* **47** (1986), 741-747.

Department of Mathematics, University of Southern California, Los Angeles, CA 90089-2532
E-mail address: fulman@usc.edu

School of Mathematics, University of Minnesota, Minneapolis, MN 55455
E-mail address: stanton@math.umn.edu