CONVERGENCE RATES OF RANDOM WALK ON IRREDUCIBLE REPRESENTATIONS OF FINITE GROUPS

JASON FULMAN

Abstract. Random walk on the set of irreducible representations of a finite group is investigated. For the symmetric and general linear groups, a sharp convergence rate bound is obtained and a cutoff phenomenon is proved. As related results, an asymptotic description of Plancherel measure of the finite general linear groups is given, and a connection of these random walks with the hidden subgroup problem of quantum computing is noted.

1. Introduction

The study of convergence rates of random walk on a finite group is a rich subject; three excellent surveys are [Al], [Sal] and [D1]. A crucial role is played by random walks where the generating measure is constant on conjugacy classes. An exact diagonalization of such walks is possible in terms of representation theory; this sometimes leads to sharp convergence rate bounds and even a proof of the cut-off phenomenon. Two important cases where this has been carried out are the random transposition walk on the symmetric group S_n [DSh] and the random transvection walk on the finite special linear group $SL(n,q)$ [H]. These "exactly solved" Markov chains also serve as useful base chains for which the comparison theory of [DSa] can be used to analyze many other random walks.

The current paper investigates a dual question, namely convergence rates of random walk on $Irr(G)$, the set of irreducible representations of a finite group G. Here the stationary distribution is not the uniform distribution, but the Plancherel measure π on $Irr(G)$, which assigns a representation λ probability $\frac{d_\lambda^2}{|G|}$, where d_λ denotes the dimension of λ. Letting η be a (not necessarily irreducible) representation of G whose character is real valued, one can define a Markov chain on $Irr(G)$ as follows. From an irreducible representation λ, one transitions to the irreducible representation ρ with probability

$$\frac{d_\rho m_\rho(\lambda \otimes \eta)}{d_\lambda d_\eta}$$

1991 *Mathematics Subject Classification.* 60C05, 20P05.

Key words and phrases. Markov chain, Plancherel measure, cutoff phenomenon, finite group, hidden subgroup problem, quantum computing.

First Version: July 15, 2006. Final revisions: April 13, 2007. To appear in Journal of Theoretical Probability.

where $m_\rho(\lambda \otimes \eta)$ denotes the multiplicity of ρ in the tensor product (also called the Kronecker product) of λ and η. Letting χ denote the character of a representation, the formula

$$m_\rho(\lambda \otimes \eta) = \frac{1}{|G|} \sum_{g \in G} \chi^\rho(g) \chi^\eta(g) \overline{\chi^\lambda(g)}$$

immediately implies that this Markov chain is reversible with respect to the Plancherel measure π.

Since these Markov chains are almost completely unexplored, we give a detailed list of motivation for why they are worth studying:

(1): The same transition mechanism on $Irr(G)$ has been studied in the closely related case where G is a compact Lie group or a Lie algebra, instead of a finite group. Then the state space $Irr(G)$ is infinite so the questions are of a different nature than those in the current paper. If $G = SU(2)$, then $Irr(G)$ is equal to the integers, and the paper [ER] studied asymptotics of n-step transition probabilities. Section 5 of [BBO] used random walk on $Irr(G)$ in the Lie algebra case, together with the Littelmann path model, to construct Brownian motion on a Weyl chamber.

(2): Decomposing the tensor product of two elements of $Irr(G)$ (which is what a step in the random walk on $Irr(G)$ does) is just as natural as decomposing the product of two conjugacy classes of G (which is what a step in usual random walk on G does). One case when tensor products are known to have an attractive combinatorial formulation is when G is a finite subgroup of $SU(2,\mathbb{C})$ and η is the natural representation; then it follows from McKay's work [Mc] that random walk on $Irr(G)$ becomes random walk on affine Dynkin diagrams.

For abelian groups, $Irr(G)$ is isomorphic to G, and random walk on $Irr(G)$ is equivalent to random walk on G. For example the usual nearest neighbor walk on the circle ($G = \mathbb{Z}_n$) is obtained by letting η be the average of the representation closest to the trivial representation and its inverse, so that $\chi^\eta(j) = cos\left(\frac{2\pi j}{n}\right)$.

Another remark which supports the idea of thinking of random walk on G and random walk on $Irr(G)$ as "dual" is the following. Whereas the eigenvalues of random walk on G generated by a conjugacy classes C are $\frac{\chi^\lambda(C)}{d_\lambda}$ where C is fixed and λ varies [DSh], the eigenvalues of random walk on $Irr(G)$ determined by the representation η are $\frac{\chi^\eta(C)}{d_\eta}$ where η is fixed and C varies [F2].

(3): Decomposing the tensor product of irreducible representations of a finite group G is useful in quantum computing: see for instance [K] or page 7 of [MR], where the transition mechanism on $Irr(G)$ is called the natural distribution of ρ in $\lambda \otimes \eta$. There are also interesting connections to free probability theory (Theorems 1.4.1 and 1.4.2 of [B1]).

(4): Combinatorialists have studied the decomposition of the r-fold tensor product of a fixed element of $Irr(G)$, when G is a finite group. Some recent results appear in [GC] and [GK]. Our previous papers [F1], [F3] used convergence rates of random walk on $Irr(G)$ to study the decomposition of tensor products. The current paper gives sharp convergence rate bounds in some cases and so better results. It should also be noted that if G is a Lie algebra, there has been nice work done on the decomposition of the r-fold tensor product of a fixed element of $Irr(G)$ ([B2], [GM], [TZ]).

(5): There are dozens of papers written about the Plancherel measure of the symmetric group (see the seminal papers [J], [O], [BOO] and the references therein). To prove results about a probability distribution π of interest, it is useful to have a Markov chain which is reversible with respect to π, and which can be completely analyzed. For instance the papers [F1],[F4] used Stein's method and random walk on $Irr(G)$ to obtain the first error term for Kerov's central limit theorem for the random character ratios $\frac{|C|^{1/2}\chi^{\lambda}(C)}{d_{\lambda}}$, where C is fixed and λ is from Plancherel measure. Also, convergence rate results for a Markov chain can be used to prove concentration inequalities for the stationary distribution π [C].

(6): The Markov chains on $Irr(G)$ are a tractable testing ground for results in finite Markov chain theory. Whereas random walks on groups (such as the random transposition and random transvection walk) have simple transition probabilities but a complicated spectrum, the walks analyzed in this paper (which are dual to the random transposition and transvection walks) have complicated transition probabilities but a simple spectrum. This has the effect of making convergence rate upper bounds somewhat easier to prove, but convergence rate lower bounds somewhat harder to prove.

The organization of this paper is as follows. Section 2 gives the needed background on Markov chain theory and defines the cutoff phenomenon. Section 3 recalls the diagonalization of the Markov chains on $Irr(G)$ and develops a group theoretic tool useful for proving lower bounds. Section 4 proves sharp convergence rate results for random walk on $Irr(G)$ when G is the symmetric group and η is the defining representation (whose character on a permutation is the number of fixed points). Section 5 proves sharp convergence rate results for random walk on $Irr(G)$ when G is the finite general linear group and η is the permutation representation on the natural vector space (whose character is the number of fixed vectors). Section 6 obtains an elegant asymptotic description of the Plancherel measure of $GL(n,q)$ (the next case to be understood after the well studied case of the symmetric groups). Also, a connection with the proof of the convergence rate lower bound of Section 5 is noted. The paper closes with the very brief Section 7, which uses random walk on $Irr(G)$ to explain (and slightly sharpen) a lemma used in work on the hidden subgroup problem of quantum computing.

The follow-up paper [F7] determines exact convergence rate asymptotics for the walks in this paper when one uses separation distance instead of total variation distance. It should also be noted that the methods of this paper extend to other algebraic and combinatorial structures, such as spherical functions of Gelfand pairs, and Bratteli diagrams. This will be treated in a sequel.

2. Preliminaries on Markov chain theory

This section collects some background on finite Markov chains. Let X be a finite set and K a matrix indexed by $X \times X$ whose rows sum to 1. Let π be a distribution such that K is reversible with respect to π; this means that $\pi(x)K(x,y) = \pi(y)K(y,x)$ for all x, y and implies that π is a stationary distribution for the Markov chain corresponding to K. Define the inner product space $L^2(\pi)$ by letting $\langle f, g\rangle = \sum_{x \in X} f(x)g(x)\pi(x)$ for real functions f, g. Then when K is considered as an operator on $L^2(\pi)$ by

$$Kf(x) := \sum_y K(x,y)f(y),$$

it is self adjoint. Hence K has an orthonormal basis of eigenvectors $f_i(x)$ with $Kf_i(x) = \beta_i f_i(x)$, where both f_i and β_i are real. It is easily shown that the eigenvalues satisfy $-1 \leq \beta_{|X|-1} \leq \cdots \leq \beta_1 \leq \beta_0 = 1$.

Recall that the total variation distance between probabilities P, Q on X is defined as $||P - Q|| = \frac{1}{2}\sum_{x \in X} |P(x) - Q(x)|$. It is not hard to see (and will be used later in proving lower bounds), that

$$||P - Q|| = \max_{A \subseteq X} |P(A) - Q(A)|.$$

Let K_x^r be the probability measure given by taking r steps from the starting state x. We will be interested in the behavior of $||K_x^r - \pi||$.

The following lemma is well known. Part 1 is the usual method for computing the power of a diagonalizable matrix. Part 2 upper bounds $||K_x^r - \pi||$ in terms of eigenvalues and eigenvectors and seems to be remarkably effective in many examples. See [DH] for a proof of part 2.

Lemma 2.1.

(1) *$K^r(x,y) = \sum_{i=0}^{|X|-1} \beta_i^r f_i(x) f_i(y)\pi(y)$ for any $x, y \in X$.*

(2)

$$4||K_x^r - \pi||^2 \leq \sum_y \frac{|K^r(x,y) - \pi(y)|^2}{\pi(y)} = \sum_{i=1}^{|X|-1} \beta_i^{2r} |f_i(x)|^2.$$

Note that the final sum does not include $i = 0$.

Finally, let us give a precise definition of the cutoff phenomenon, taken from [Sal]. Consider a family of finite sets X_n, each equipped with a stationary distribution π_n, and with another probability measure p_n that induces a random walk on X_n. We say that the cutoff phenomenon holds for the family (X_n, π_n) if there exists a sequence (t_n) of positive reals such that

(1) $\lim_{n\to\infty} t_n = \infty$;
(2) For any $\epsilon \in (0,1)$ and $r_n = [(1+\epsilon)t_n]$, $\lim_{n\to\infty} ||p_n^{r_n} - \pi_n|| = 0$;
(3) For any $\epsilon \in (0,1)$ and $r_n = [(1-\epsilon)t_n]$, $\lim_{n\to\infty} ||p_n^{r_n} - \pi_n|| = 1$.

The paper [D2] is a nice survey of the cutoff phenomenon.

3. Preliminaries on group theory

This section collects and develops some useful group theoretic information. Throughout K is the Markov chain on $Irr(G)$ defined using a representation η (not necessarily irreducible) whose character is real valued.

Lemma 3.1. *(*[F2]*, Proposition 2.3) The eigenvalues of K are indexed by conjugacy classes C of G:*

(1) *The eigenvalue parameterized by C is $\frac{\chi^\eta(C)}{d_\eta}$.*
(2) *An orthonormal basis of eigenfunctions f_C in $L^2(\pi)$ is defined by $f_C(\rho) = \frac{|C|^{1/2}\chi^\rho(C)}{d_\rho}$.*

Lemma 3.2 relates the transition probabilities of K to the decomposition of tensor products. This will be useful in proving the lower bound for the convergence rate of K when the group is $GL(n,q)$.

Lemma 3.2. *Let $\hat{1}$ denote the trivial representation of G. Then*

$$K^r(\hat{1}, \rho) = \frac{d_\rho}{d_\eta^r} m_\rho(\eta^r),$$

where $m_\rho(\eta^r)$ denotes the multiplicity of ρ in η^r.

Proof. Lemma 3.1 and part 1 of Lemma 2.1 imply that

$$\begin{aligned} K^r(\hat{1}, \rho) &= \sum_C \left(\frac{\chi^\eta(C)}{d_\eta}\right)^r f_C(\hat{1}) f_C(\rho)\pi(\rho) \\ &= \sum_C \left(\frac{\chi^\eta(C)}{d_\eta}\right)^r |C| \frac{\chi^\rho(C)}{d_\rho} \frac{d_\rho^2}{|G|} \\ &= \frac{d_\rho}{d_\eta^r} \frac{1}{|G|} \sum_g \chi^\eta(g)^r \chi^\rho(g). \end{aligned}$$

The result now follows since χ^η is real valued. □

Finally, we derive a result which should be useful in many examples for lower bounding the convergence rate of the Markov chain K. It will be applied in Section 4.

Proposition 3.3. *Let C be a conjugacy class of G satisfying $C = C^{-1}$ and let f_C be as in Lemma 3.1. Let $\mathbb{E}_{K^r}[(f_C)^s]$ denote the expected value of $(f_C)^s$ after r steps of the random walk K started at the trivial representation. Let*

$p_{s,C}(T)$ be the probability that the random walk on G generated by C and started at the identity is in the conjugacy class T after s steps. Then

$$\mathbb{E}_{K^r}[(f_C)^s] = |C|^{s/2} \sum_T p_{s,C}(T) \left(\frac{\chi^\eta(T)}{d_\eta} \right)^r ,$$

where the sum is over all conjugacy classes T of G.

Proof. Let $\hat{1}$ denote the trivial representation of G. It follows from Lemma 3.1 and part 1 of Lemma 2.1 that

$$\begin{aligned}
\mathbb{E}_{K^r}[(f_C)^s] &= \sum_\rho K^r(\hat{1},\rho) f_C(\rho)^s \\
&= \sum_\rho \sum_T \left(\frac{\chi^\eta(T)}{d_\eta} \right)^r f_T(\hat{1}) f_T(\rho) \frac{d_\rho^2}{|G|} f_C(\rho)^s \\
&= \sum_\rho \sum_T \left(\frac{\chi^\eta(T)}{d_\eta} \right)^r \frac{|T|}{|G|} d_\rho^2 \frac{\chi^\rho(T)}{d_\rho} \left(\frac{|C|^{1/2}\chi^\rho(C)}{d_\rho} \right)^s \\
&= |C|^{s/2} \sum_T \left(\frac{\chi^\eta(T)}{d_\eta} \right)^r \frac{|T|}{|G|} \sum_\rho d_\rho^2 \frac{\chi^\rho(T)}{d_\rho} \left(\frac{\chi^\rho(C)}{d_\rho} \right)^s .
\end{aligned}$$

To complete the proof we use the fact that

$$p_{s,C}(T) = \frac{|T|}{|G|} \sum_\rho d_\rho^2 \frac{\chi^\rho(T)}{d_\rho} \left(\frac{\chi^\rho(C)}{d_\rho} \right)^s .$$

This is the standard Fourier analytic expression for $p_{s,C}(T)$; it is explicitly stated as Exercise 7.67 of [St2] and also follows from Chapter 2 of [D1]. □

4. The symmetric group

The primary purpose of this section is to obtain sharp convergence rates and a cutoff phenomenon for random walk on $Irr(S_n)$ when η is the defining representation of S_n, whose character on a permutation is the number of fixed points. Subsection 4.1 states and discusses the main result, as well as other interesting interpretations of the random walk (none of which will be needed for the proof of the main result). The main result is proved in Subsection 4.2.

4.1. **Main result: statement and discussion.**

The following theorem is the main result in this paper concerning random walk on $Irr(S_n)$. For its statement, recall from Section 2 that the total variation distance $||P-Q||$ between two probability distributions P,Q on a finite set X is defined as $\frac{1}{2}\sum_{x \in X} |P(x)-Q(x)|$. Also note that Theorem 4.1 proves a cutoff phenomenon (as defined in Section 2) for the random walk.

Theorem 4.1. *Let G be the symmetric group S_n and let π be the Plancherel measure of G. Let η be the n-dimensional defining representation of S_n. Let*

K^r denote the distribution of random walk on $Irr(G)$ after r steps, started from the trivial representation.

(1) *If $r = \frac{1}{2}n\log(n) + cn$ with $c \geq 1$ then*

$$||K^r - \pi|| \leq \frac{e^{-2c}}{2}.$$

(2) *If $r = \frac{1}{2}n\log(n) - cn$ with $0 \leq c \leq \frac{1}{6}\log(n)$, then there is a universal constant a (independent of c, n) so that*

$$||K^r - \pi|| \geq 1 - ae^{-4c}.$$

It is well known [Sag] that the irreducible representations of S_n correspond to partitions of n, with the trivial representation corresponding to the one-row partition of size n. Thus it is natural to ask whether the random walk of Theorem 4.1 has a simple combinatorial description. Proposition 4.2 (which was implicit in [F1]) shows that it does.

Proposition 4.2. *A step in the random walk of Theorem 4.1 has the following combinatorial description on partitions of n. From a partition λ, first one moves to a partition μ of size $n-1$ which can be obtained by removing a corner box from λ; the chance of moving to μ is $\frac{d_\mu}{d_\lambda}$. Then one moves from μ to a partition ρ of size n by adding a corner box to μ; the chance of moving to ρ is $\frac{d_\rho}{nd_\mu}$.*

Proof. By definition, the chance of moving from λ to ρ is $\frac{d_\rho}{nd_\lambda}$ multiplied by the multiplicity of ρ in $\lambda \otimes \eta$, where η is the n-dimensional defining representation of S_n. Lemma 3.5 of [F1] shows that $\lambda \otimes \eta$ is equal to the representation of S_n obtained by restricting λ to S_{n-1} and then inducing it to S_n. Thus the branching rules for restriction and induction in the symmetric group [Sag] imply that the multiplicity of ρ in $\lambda \otimes \eta$ is the number of μ of size $n-1$ which can be obtained from both of λ, ρ by removing some corner box (this number is at most 1 if $\lambda \neq \rho$). The result follows. □

Remark: Theorem 3.1 of [F3] gave yet another description of the random walk on partitions of n corresponding to the walk on $Irr(S_n)$ in Theorem 4.1. It proved that the partition corresponding to a representation chosen from K^r has the same distribution as the Robinson-Schensted-Knuth (RSK) shape of a permutation obtained after r iterations of the top to random shuffle. Hence Theorem 4.1 determines the precise convergence rate of this RSK shape; note that it is faster than that of the top to random shuffle, which takes $n\log(n) + cn$ steps to become random. The reader may wonder why one would care about such statistics, but the distribution of the RSK shape of a permutation after various shuffling methods is interesting (see [F6] for more discussion, including an explanation of why Johansson's work on discrete orthogonal polynomial ensembles [J] determines the convergence rate of the RSK shape after riffle shuffles).

To close the discussion of Theorem 4.1, it is interesting to compare it with the following classic result on the random transposition walk on S_n.

Theorem 4.3. ([DSh]) *Consider random walk on the symmetric group S_n, where at each step two symbols are chosen uniformly at random (possibly the same symbol), and are transposed. If $r = \frac{1}{2}\log(n) + cn$ with $c > 0$, then after r iterations the total variation distance to the uniform distribution is at most ae^{-2c} for a universal constant a. Moreover, for $c < 0$, as $n \to \infty$, the total variation distance to the uniform distribution is at least $(\frac{1}{e} - e^{-e^{-2c}}) + o(1)$.*

Theorems 4.1 and 4.3 establish cutoffs for the random walks in question, and there is a close parallel between them. The convergence rates are essentially the same, and whereas Theorem 4.3 is based on the class of transpositions, which is the conjugacy class closest to the identity, Theorem 4.1 is based on the defining representation, which decomposes into the trivial representation and the representation closest to the trivial representation.

4.2. **Proof of Theorem 4.1.**

The purpose of this subsection is to prove Theorem 4.1. Lemma 4.4 is useful for proving the upper bound in Theorem 4.1.

Lemma 4.4. *Suppose that $0 \leq i \leq n-2$. Then the number of permutations on n symbols with exactly i fixed points is at most $\frac{1}{2}\frac{n!}{i!}$.*

Proof. The number of permutations on n symbols with exactly i fixed points is $\binom{n}{i} d_{n-i}$ where d_m denotes the number of permutations on m symbols with no fixed points. It follows from the principle of inclusion-exclusion (see page 67 of [St1]) that

$$d_m = m! \left(1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \cdots + (-1)^m \frac{1}{m!}\right).$$

Thus $d_m \leq \frac{m!}{2}$ if $m \geq 2$, which implies the result. □

Now the upper bound in Theorem 4.1 can be proved.

Proof. (Of part 1 of Theorem 4.1) From Lemma 3.1 and part 2 of Lemma 2.1 it follows that

$$4||K^r - \pi||^2 \leq \sum_{i=0}^{n-2} |\{g \in S_n : fp(g) = i\}| \left(\frac{i}{n}\right)^{2r}$$

where $fp(g)$ is the number of fixed points of g. Note that the sum ends at $n-2$ since no permutation can exactly have $n-1$ fixed points. Applying

Lemma 4.4 and then letting $j = n - i$, one concludes that

$$\begin{aligned} 4||K^r - \pi||^2 &\leq \frac{1}{2}\sum_{i=0}^{n-2} \frac{n!}{i!}\left(\frac{i}{n}\right)^{2r} \\ &= \frac{1}{2}\sum_{j=2}^{n} \frac{n!}{(n-j)!}\left(1-\frac{j}{n}\right)^{2r} \\ &= \frac{1}{2}\sum_{j=2}^{n} \frac{n!}{(n-j)!}e^{2r\cdot\log(1-j/n)} \\ &\leq \frac{1}{2}\sum_{j=2}^{n} \frac{n!}{(n-j)!}e^{-2rj/n}. \end{aligned}$$

Recalling that $r = \frac{1}{2}n\log(n) + cn$, the bound becomes

$$\frac{1}{2}\sum_{j=2}^{n} \frac{n!}{(n-j)!n^j}e^{-2cj} \leq \frac{1}{2}\sum_{j=2}^{n} e^{-2cj} = \frac{e^{-4c}}{2(1-e^{-2c})}.$$

Dividing by 4 and taking square roots, the result follows since $c \geq 1$. □

The idea for proving the lower bound of Theorem 4.1 will be to find a random variable on $Irr(G)$ which is far from its distribution under Plancherel measure if fewer than $\frac{1}{2}n\log(n)$ steps have been taken. The random variable to be used is precisely the f_C from Lemma 3.1, where C is the conjugacy class of transpositions. This approach is dual to, and motivated by, the approach on page 44 of [D1] for proving the lower bound in Theorem 4.3.

Proof. (Of part 2 of Theorem 4.1). We apply Chebyshev's inequality. Let C be the conjugacy class of transpositions, and let f_C be as in Lemma 3.1. For $\alpha > 0$ to be specified later, let A be the event that $f_C \leq \alpha$. The orthogonality relations for the irreducible characters of the symmetric group imply that under Plancherel measure π, the random variable f_C has mean 0 and variance 1. Hence $\pi(A) \geq 1 - \frac{1}{\alpha^2}$.

On the other hand, it follows from Proposition 3.3 that

$$\mathbb{E}_{K^r}[f_C] = \sqrt{\binom{n}{2}}\left(1-\frac{2}{n}\right)^r.$$

Letting $r = \frac{1}{2}n\log(n) - cn$ and using the Taylor expansion for $\log(1-x)$ gives that

$$\begin{aligned}
\mathbb{E}_{K^r}[f_C] &= \sqrt{\binom{n}{2}} \exp\left((\frac{1}{2}n\log(n) - cn) \cdot \log(1-2/n) \right) \\
&= \sqrt{\binom{n}{2}} \exp\left(-\log(n) + 2c + O(\frac{\log(n)}{n}) + O(\frac{c}{n}) \right) \\
&\geq \frac{1}{2} \exp\left(2c + O(\frac{\log(n)}{n}) + O(\frac{c}{n}) \right).
\end{aligned}$$

This is large when c is large.

Proposition 3.3 gives that

$$\mathbb{E}_{K^r}[(f_C)^2] = 1 + \binom{n-2}{2}(1-\frac{4}{n})^r + (2n-4)(1-\frac{3}{n})^r.$$

Thus the variance of f_C under K^r is

$$\begin{aligned}
& 1 + \binom{n-2}{2}(1-\frac{4}{n})^r + (2n-4)(1-\frac{3}{n})^r - \binom{n}{2}(1-\frac{2}{n})^{2r} \\
= \; & 1 + \binom{n-2}{2} \exp\left((\frac{1}{2}n\log(n) - cn)(-\frac{4}{n} + O(\frac{1}{n^2})) \right) \\
& +(2n-4) \exp\left((\frac{1}{2}n\log(n) - cn)(-\frac{3}{n} + O(\frac{1}{n^2})) \right) \\
& -\binom{n}{2} \exp\left((n\log(n) - 2cn)(-\frac{2}{n} + O(\frac{1}{n^2})) \right) \\
= \; & 1 + \frac{1}{2} \exp\left(4c + O(\frac{\log(n)}{n}) + O(\frac{c}{n}) \right) \\
& +\frac{2}{\sqrt{n}} \exp\left(3c + O(\frac{\log(n)}{n}) + O(\frac{c}{n}) \right) \\
& -\frac{1}{2} \exp\left(4c + O(\frac{\log(n)}{n}) + O(\frac{c}{n}) \right) \\
= \; & 1 + \frac{e^{4c}}{2} \left(O(\frac{\log(n)}{n}) + O(\frac{c}{n}) \right) + \frac{2}{\sqrt{n}} \exp\left(3c + O(\frac{\log(n)}{n}) + O(\frac{c}{n}) \right).
\end{aligned}$$

Since $0 \leq c \leq \frac{1}{6}\log(n)$, the variance is bounded by a universal constant. Let $\alpha = \frac{e^{2c}}{4}$. Then Chebyshev's inequality gives that $K^r(A) \leq \frac{b}{e^{4c}}$ for a universal constant b. Thus

$$||K^r - \pi|| \geq |\pi(A) - K^r(A)| \geq 1 - \frac{1}{\alpha^2} - \frac{b}{e^{4c}},$$

which completes the proof. □

5. The general linear group

This section studies random walk on $Irr(GL(n,q))$ in the case that η is the representation of $GL(n,q)$ whose character is $q^{d(g)}$, where $d(g)$ is the dimension of the fixed space of g. Subsection 5.1 states and discusses the main result. Subsection 5.2 proves the upper bound in Theorem 5.1 and Subsection 5.3 proves the lower bound.

5.1. **Main result: statement and discussion.** The following theorem is the main result in the paper concerning random walk on $Irr(GL(n,q))$.

Theorem 5.1. *Let G be the finite general linear group $GL(n,q)$ and let π be the Plancherel measure of G. Let η be the representation of G whose character is $q^{d(g)}$, where $d(g)$ is the dimension of the fixed space of g. Let K^r denote the distribution of random walk on $Irr(G)$ after r steps started from the trivial representation.*

(1) *If $r = n + c$ with $c > 0$, then $||K^r - \pi|| \leq \frac{1}{2q^c}$.*
(2) *If $r = n - c$ with $c > 0$, then $||K^r - \pi|| \geq 1 - \frac{a}{q^c}$ where a is a universal constant (independent of n, q, c).*

It is interesting to compare this result with the following result of Hildebrand on the random transvection walk.

Theorem 5.2. ([H]) *Consider random walk on the finite special linear group $SL(n,q)$, where at each step one multiplies by a random transvection (i.e. an element of $SL(n,q)$ which is not the identity but fixes all points in a hyperplane). There are positive constants a, b such that for sufficiently large n and all $c > 0$, the total variation distance to the uniform distribution after $n + c$ steps is at most ae^{-bc}. Moreover, given $\epsilon > 0$, there exists $c > 0$ so that the total variation distance is at least $1 - \epsilon$ after $n - c$ iterations for sufficiently large n.*

In both theorems there is a cutoff around n steps. Also, whereas Theorem 5.2 is based on the class of transvections, which is the unipotent class closest to the identity, Theorem 5.1 is based on a representation which for $q = 2$ decomposes into the trivial representation and the unipotent representation closest to the trivial representation (for $q > 2$ the decomposition involves a few more pieces).

5.2. **Upper bound on convergence rate.** To prove the upper bound of Theorem 5.1, the following lemma will be helpful. Recall that $d(g)$ is the dimension of the fixed space of g. We also use the notation that $(1/q)_r = (1 - 1/q) \cdots (1 - 1/q^r)$.

Lemma 5.3. *Suppose that $0 \leq i \leq n$. Then the number of elements in $GL(n,q)$ with $d(g) = i$ is at most $q^{n^2 - i^2}$.*

Proof. It is known (going back at least to [RS]) that the number of elements in $GL(n,q)$ with $d(g)=i$ is exactly

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

Since $|GL(n,q)|=q^{n^2}(1/q)_n$, clearly $\frac{|GL(n,q)|}{|GL(i,q)|}\leq q^{n^2-i^2}$. Also

$$\sum_{j=0}^{n-i}\frac{(-1)^j q^{\binom{j}{2}}}{q^{ij}|GL(j,q)|}=\sum_{j=0}^{n-i}\frac{(-1)^j}{q^{ij}(q^j-1)\cdots(q-1)}$$

is an alternating sum of decreasing terms the first of which is 1, so the sum is at most 1. This proves the lemma. □

Proof. (Of part 1 of Theorem 5.1) By Lemma 3.1 and part 2 of Lemma 2.1, it follows that

$$\begin{aligned}4||K^r-\pi||^2 &\leq \sum_{i=0}^{n-1}|\{g\in GL(n,q):d(g)=i\}|\left(\frac{1}{q^{n-i}}\right)^{2r}\\ &= \sum_{i=1}^{n}|\{g\in GL(n,q):d(g)=n-i\}|\left(\frac{1}{q^{i}}\right)^{2r},\end{aligned}$$

where $d(g)$ is the dimension of the fixed space of g. By Lemma 5.3 this is at most $\sum_{i=1}^{n}\frac{q^{2ni}}{q^{i^2+2ir}}$. Since $r=n+c$, this is equal to

$$\sum_{i=1}^{n}\frac{1}{q^{i^2+2ci}}\leq q^{-2c}\sum_{i=1}^{n}\frac{1}{q^{i^2}}\leq\frac{1}{q(1-1/q)}q^{-2c}.$$

Since $q\geq 2$, this is at most q^{-2c}. Dividing by 4 and taking square roots completes the proof. □

5.3. **Lower bound on convergence rate.** To prove the lower bound of Theorem 5.1, we will need to know about representation theory of $GL(n,q)$ and about the decomposition of η^k into irreducibles, where $1\leq k\leq n$. In fact the paper [GK] studies this decomposition.

To begin we recall some facts about $Irr(GL(n,q))$. A full treatment of the subject with proofs appears in [Ma], [Z] but we will adhere to the notation of [GK] instead. As usual a partition $\lambda=(\lambda_1,\cdots,\lambda_m)$ is identified with its geometric image $\{(i,j):1\leq i\leq m,1\leq j\leq\lambda_i\}$ and $|\lambda|=\lambda_1+\cdots+\lambda_m$ is the total number of boxes. We also use that notation that λ' is the transpose of λ, obtained by switching the rows and columns of λ (i.e. $\lambda'_i=|\{j:\lambda_j\geq i\}|$). Let $\mathbb{Y}$ denote the set of all partitions, including the empty partition of size 0.

In what follows C_d denotes the set of cuspidal characters of $GL(d,q)$. The precise definition of a cuspidal character is not needed but we remark that $|C_d|=\frac{1}{d}\sum_{r|d}\mu(r)(q^{d/r}-1)$. Let $C=\bigcup_{d\geq 1}C_d$. The unit character of

$GL(1,q)$ plays an important role and will be denoted e; it is one of the $q-1$ elements of C_1. Given a family $\phi : C \mapsto \mathbb{Y}$ with finitely many non-empty partitions $\phi(c)$, its degree $||\phi||$ is defined as $\sum_{d\geq 1}\sum_{c\in C_d} d\cdot|\phi(c)|$. We also write $||c|| = d$ if d is the unique number so that $c \in C_d$. A fundamental result is that the irreducible representations of $GL(n,q)$ are in bijection with the families of partitions of degree n, so we also let ϕ denote the corresponding representation. The partition $\phi(e)$ will be referred to as the unipotent part of ϕ.

It will be helpful to know that the dimension of the irreducible representation of $GL(n,q)$ corresponding to the family ϕ is

$$(q^n-1)\cdots(q-1)\prod_{d\geq 1}\prod_{c\in \mathcal{C}_d}\frac{q^{d\cdot n(\phi(c))}}{\prod_{b\in\phi(c)}(q^{d\cdot h(b)}-1)},$$

where $h(b)$ is the hooklength $\lambda_i + \lambda'_j - i - j + 1$ of a box $b = (i,j)$ and $n(\lambda) = \sum_i (i-1)\lambda_i$.

Proposition 5.4. *Suppose that $K^r(\hat{1},\phi) > 0$. Then $\phi(e)_1 \geq n-r$.*

Proof. If $r = 0$ or $r > n$ the result is trivially true (and not useful to us). So suppose that $1 \leq r \leq n$. Lemma 3.2 implies that $K^r(\hat{1},\phi) > 0$ if and only if ϕ occurs as a component of η^r. Proposition 5 and Theorem 7 of [GK] imply that if $1 \leq r \leq n$ and ϕ occurs as a component of η^r, then $\phi(e)_1 \geq n-r$. □

For $c > 0$, define A as the event that a representation has the first row of its unipotent part of size at least c. Proposition 5.4 showed that if $r = n-c$, then $K^r(A) = 1$. The next goal will be to upper bound $\pi(A)$ where π is the Plancherel measure of $GL(n,q)$. First we upper bound the Plancherel probability that the unipotent part of a random representation is λ.

Lemma 5.5. *Let π be the Plancherel measure of $GL(n,q)$. Then for any λ,*

$$\pi(\phi(e)=\lambda) \leq \frac{1}{q^{\sum_i(\lambda_i)^2}\prod_{b\in\lambda}(1-1/q^{h(b)})^2}.$$

Proof. By the definition of Plancherel measure and the formula for d_ϕ one has that

$$\begin{aligned}
\pi(\phi(e)=\lambda) &= \sum_{\substack{||\phi||=n\\ \phi(e)=\lambda}} \frac{d_\phi^2}{|GL(n,q)|}\\
&= \frac{(q^n-1)\cdots(q-1)}{q^{\binom{n}{2}}} \sum_{\substack{||\phi||=n\\ \phi(e)=\lambda}} \prod_{d\geq 1}\prod_{c\in C_d} \frac{q^{2d\cdot n(\phi(c))}}{\prod_{b\in\phi(c)}(q^{d\cdot h(b)}-1)^2}\\
&= \frac{q^{n+2n(\lambda)}(1/q)_n}{\prod_{b\in\lambda}(q^{h(b)}-1)^2} \sum_{\substack{||\phi||=n-|\lambda|\\ \phi(e)=\emptyset}} \prod_{d\geq 1}\prod_{c\in C_d} \frac{q^{2d\cdot n(\phi(c))}}{\prod_{b\in\phi(c)}(q^{d\cdot h(b)}-1)^2}\\
&\leq \frac{q^{n+2n(\lambda)}(1/q)_n}{\prod_{b\in\lambda}(q^{h(b)}-1)^2} \sum_{||\phi||=n-|\lambda|} \prod_{d\geq 1}\prod_{c\in C_d} \frac{q^{2d\cdot n(\phi(c))}}{\prod_{b\in\phi(c)}(q^{d\cdot h(b)}-1)^2}\\
&= \frac{q^{n+2n(\lambda)}(1/q)_n}{\prod_{b\in\lambda}(q^{h(b)}-1)^2} \sum_{||\phi||=n-|\lambda|} \frac{d_\phi^2}{(q^{n-|\lambda|}-1)^2\cdots(q-1)^2}.
\end{aligned}$$

Since the sum of the squares of the dimensions of the irreducible representations of a finite group is equal to the order of the group, this is

$$\begin{aligned}
& \frac{q^{n+2n(\lambda)}(1/q)_n}{\prod_{b\in\lambda}(q^{h(b)}-1)^2} \frac{|GL(n-|\lambda|,q)|}{(q^{n-|\lambda|}-1)^2\cdots(q-1)^2}\\
&= \frac{q^{2n(\lambda)+|\lambda|}(1/q)_n}{(1/q)_{n-|\lambda|}\prod_{b\in\lambda}(q^{h(b)}-1)^2}\\
&\leq \frac{q^{2n(\lambda)+|\lambda|}}{\prod_{b\in\lambda}(q^{h(b)}-1)^2}\\
&= \frac{1}{q^{|\lambda|+2n(\lambda')}\prod_{b\in\lambda}(1-1/q^{h(b)})^2}\\
&= \frac{1}{q^{\sum_i(\lambda_i)^2}\prod_{b\in\lambda}(1-1/q^{h(b)})^2}.
\end{aligned}$$

The second to last equation used the identity

$$\sum_{b\in\lambda} h(b) = n(\lambda)+n(\lambda')+|\lambda|$$

on page 11 of [Ma]. □

Proposition 5.6. *There is a universal constant a (independent of n,q,c) so that $\pi(|\phi(e)|\geq c)\leq \frac{a}{q^c}$.*

Proof. By Lemma 5.5,

$$\sum_{|\lambda|=m} \pi(\phi(e)=\lambda) \leq \sum_{|\lambda|=m} \frac{1}{q^{\sum_i(\lambda_i)^2}\prod_{b\in\lambda}(1-1/q^{h(b)})^2}.$$

Noting that this sum is invariant under transposing λ, Proposition 4.2 of [F5] implies that it is equal to the coefficient of u^m in $\prod_{i=1}^{\infty} \prod_{j=0}^{\infty} \left(\frac{1}{1-\frac{u}{q^{i+j}}} \right)$. Lemma 4.4 of [F5] shows that since $q \geq 2$, this coefficient is at most $\frac{1}{(q^m-1)(1-1/q)^6}$. Thus

$$\pi(|\phi(e)| \geq c) = \sum_{m \geq c} \pi(|\phi(e)| = m) \leq \frac{1}{(1-1/q)^6} \sum_{m \geq c} \frac{1}{q^m - 1},$$

which implies the result. □

The lower bound of Theorem 5.1 can now be proved.

Proof. (Of part 2 of Theorem 5.1). Fix $c > 0$ and define A as the event that a representation has the first row of its unipotent part of size at least c. Defining $r = n - c$, Proposition 5.4 showed that $K^r(A) = 1$. Clearly $\pi(A) \leq \pi(|\phi(e)| \geq c)$. By Proposition 5.6, this is at most $\frac{a}{q^c}$ for a universal constant a. Since $||K^r - \pi|| \geq |K^r(A) - \pi(A)|$, the result follows. □

6. Asymptotic description of Plancherel measure of $GL(n,q)$

Given the numerous papers on asymptotics of Plancherel measure of the symmetric groups (see [J],[O],[BOO] and references therein), it is natural to study asymptotics of Plancherel measure for other towers of finite groups. Aside from the paper [VK], which is only tangentially related and contains no proofs, we are aware of no results on this question. In this section an elegant asymptotic description of the Plancherel measure of $GL(n,q)$ is obtained, when q is fixed and $n \to \infty$: it is proved that this limiting measure factors into independent pieces, the distributions of which can be explicitly described. Then a connection with the proof of the convergence rate lower bound of Theorem 5.1 is noted.

Fix $c \in \mathcal{C}$ and let ϕ be a representation chosen from the Plancherel measure π of $GL(n,q)$. Then the partition $\phi(c)$ is a random partition (of size at most n). It is natural to study the distribution of $\phi(c)$ when c is fixed and $n \to \infty$. Theorem 6.3 will show that the random partitions $\{\phi(c) : c \in \mathcal{C}\}$ are independent in the $n \to \infty$ limit, and will determine the distribution of each of them.

First, we define a "cycle index" $\hat{Z}_{GL(n,q)}$ for irreducible representations. For $n \geq 1$, let

$$\hat{Z}_{GL(n,q)} = \sum_{\phi:||\phi||=n} \pi(\phi) \prod_{c \in \mathcal{C}:|\phi(c)| \neq 0} x_{c,\phi(c)}.$$

Here the $x_{c,\phi(c)}$ are variables corresponding to pairs of elements of $\mathcal{C}$ and partitions.

Lemma 6.1.

$$1+\sum_{n=1}^{\infty}\hat{Z}_{GL(n,q)}\frac{u^n}{(1/q)_n}=\prod_{d\geq 1}\prod_{c\in\mathcal{C}_d}\left[1+\sum_{|\lambda|\geq 1}\frac{x_{c,\lambda}\cdot u^{d|\lambda|}}{q^{d\sum_i(\lambda_i)^2}\prod_{b\in\lambda}(1-1/q^{d\cdot h(b)})^2}\right]$$

Proof. From the formula for the dimension of an element of $Irr(GL(n,q))$ given in Subsection 5.3, it follows by comparing the coefficients of products of the x variables on both sides that

$$1+\sum_{n=1}^{\infty}\hat{Z}_{GL(n,q)}\frac{u^n}{q^n(1/q)_n}=\prod_{d\geq 1}\prod_{c\in\mathcal{C}_d}\left[1+\sum_{|\lambda|\geq 1}\frac{x_{c,\lambda}\cdot u^{d|\lambda|}q^{2d\cdot n(\lambda)}}{\prod_{b\in\lambda}(q^{d\cdot h(b)}-1)^2}\right].$$

Replacing u by uq gives that

$$1+\sum_{n=1}^{\infty}\hat{Z}_{GL(n,q)}\frac{u^n}{(1/q)_n}=\prod_{d\geq 1}\prod_{c\in\mathcal{C}_d}\left[1+\sum_{|\lambda|\geq 1}\frac{x_{c,\lambda}\cdot u^{d|\lambda|}q^{d(|\lambda|+2n(\lambda))}}{\prod_{b\in\lambda}(q^{d\cdot h(b)}-1)^2}\right].$$

Arguing as in the last two lines of the proof of Lemma 5.5 proves the result. □

To state the main result of this subsection, we define, for $q>1$ and $0<u<q$, a probability measure $S_{u,q}$ on $\mathbb{Y}$ (the set of all partitions of all natural numbers). This is defined by the formula

$$S_{u,q}(\lambda)=\prod_{i=1}^{\infty}\prod_{j=0}^{\infty}\left(1-\frac{u}{q^{i+j}}\right)\cdot\frac{u^{|\lambda|}}{q^{\sum_i(\lambda_i)^2}\prod_{b\in\lambda}(1-1/q^{h(b)})^2}.$$

This measure, and some of its properties, are discussed in [F5] (note that there λ is replaced by its transpose).

The following simple lemma is useful.

Lemma 6.2. *If a function $f(u)$ has a Taylor series around 0 which converges at $u=1$, then the $n\to\infty$ limit of the coefficient of u^n in $\frac{f(u)}{1-u}$ is equal to $f(1)$.*

Proof. Write the Taylor series $f(u)=\sum_{n=0}^{\infty}a_nu^n$. Then observe that the coefficient of u^n in $\frac{f(u)}{1-u}$ is equal to $\sum_{i=0}^{n}a_i$. □

Now the main theorem of this subsection can be proved.

Theorem 6.3. (1) *Fix u with $0<u<1$. Then choose a random natural number N with $\mathbb{P}(N=n)=\prod_{m=0}^{\infty}\left(1-\frac{u}{q^m}\right)\cdot\frac{u^n}{(1/q)_n}$. Choose ϕ from the Plancherel measure of $GL(N,q)$. Then as $c\in\mathcal{C}$ varies, the random partitions $\phi(c)$ are independent with $\phi(c)$ distributed according to the measure $S_{u^{||c||},q^{||c||}}$.*

(2) *Choose ϕ from the Plancherel measure π_n of $GL(n,q)$. Then as $n\to\infty$, the random partitions $\phi(c)$ converge to independent random variables, with $\phi(c)$ distributed according to the measure $S_{1,q^{||c||}}$.*

Proof. Setting all of the variables $x_{c,\lambda}$ equal to 1 in Lemma 6.1, the left hand side becomes $\sum_{n\geq 0}\frac{u^n}{(1/q)_n}$, which by an identity of Euler (Corollary 2.2 of [An]) is equal to $\prod_{m=0}^{\infty}(1-u/q^m)^{-1}$. Since $S_{u,q}$ is a probability measure, the right hand side becomes $\prod_{d\geq 1}\prod_{c\in\mathcal{C}_d}\prod_{i=1}^{\infty}\prod_{j=0}^{\infty}\left(1-\frac{u^d}{q^{d(i+j)}}\right)^{-1}$. Taking reciprocals of this equation and multiplying by the statement of Lemma 6.1 gives the equation

$$\begin{aligned}&\prod_{m=0}^{\infty}(1-u/q^m)+\sum_{n=1}^{\infty}\hat{Z}_{GL(n,q)}\prod_{m=0}^{\infty}(1-u/q^m)\cdot\frac{u^n}{(1/q)_n}\\ =&\prod_{d\geq 1}\prod_{c\in\mathcal{C}_d}\left(S_{u^d,q^d}(\emptyset)+\sum_{|\lambda|\geq 1}S_{u^d,q^d}(\lambda)x_{c,\lambda}\right).\end{aligned}$$

This proves the first assertion.

For the second assertion, divide both sides of the previous equation by $\prod_{m=1}^{\infty}(1-u/q^m)$, giving that

$$\begin{aligned}&(1-u)\left(1+\sum_{n=1}^{\infty}\hat{Z}_{GL(n,q)}\frac{u^n}{(1/q)_n}\right)\\ =&\prod_{m=1}^{\infty}(1-u/q^m)^{-1}\prod_{d\geq 1}\prod_{c\in\mathcal{C}_d}\left(S_{u^d,q^d}(\emptyset)+\sum_{|\lambda|\geq 1}S_{u^d,q^d}(\lambda)x_{c,\lambda}\right).\end{aligned}$$

Thus for any $c_1,\cdots,c_t\in\mathcal{C}$ and any $\lambda_1,\cdots,\lambda_t\in\mathbb{Y}$, it follows that

$$\lim_{n\to\infty}\pi_n(\phi(c_1)=\lambda_1,\cdots,\phi(c_t)=\lambda_t)$$

is equal to the limit as $n\to\infty$ of

$$(1/q)_n\cdot[u^n]\frac{1}{1-u}\prod_{m=1}^{\infty}(1-u/q^m)^{-1}\prod_{i=1}^{t}S_{u^{||c_i||},q^{||c_i||}}(\lambda_i),$$

where $[u^n]f(u)$ denotes the coefficient of u^n in $f(u)$. By Lemma 6.2 this limit exists and is $\prod_{i=1}^{t}S_{1,q^{||c_i||}}(\lambda_i)$, as desired. □

To close this section, note that part 2 of Theorem 6.3 gives an intuitive explanation of why Proposition 5.6 should be true. Indeed, $\phi(e)$ converges to a partition chosen from $S_{1,q}$ as $n\to\infty$, and a partition chosen from $S_{1,q}$ has finite size. Thus when c is big, the probability that $|\phi(e)|\geq c$ should be small.

7. Connection to the hidden subgroup problem

As is explained in Chapter 5 of the text [NC], many of the problems in which a quantum computer outperforms its classical counterpart, such as factoring and the discrete-log problem, can be described in terms of the following hidden subgroup problem. Let G be a finite group and H a subgroup. Given a function f from G to a finite set that is constant on left cosets gH of

H and takes different values for different cosets, the hidden subgroup problem is to determine a set of generators of H and the decision version of the problem is to determine whether there is a non-identity hidden subgroup or not.

One approach to these problems uses the "weak standard method" of quantum Fourier sampling, which is described in [KS] and more fully in [HRT]. The extensive survey [L] is also quite useful. When applying this to a subgroup H, one obtains a probability measure P_H on $Irr(G)$, which chooses a representation $\rho \in Irr(G)$ with probability

$$P_H(\rho) = \frac{d_\rho}{|G|} \sum_{h \in H} \chi^\rho(h).$$

Then a subgroup H can be distinguished efficiently from the trivial subgroup $\{e\}$ if and only if the total variation distance $||P_H - P_{\{e\}}||$ is larger than $(\log |G|)^{-c}$ for some constant c.

The following upper bound on the total variation distance $||P_H - P_{\{e\}}||$ was used by Kempe and Shalev in their work on the weak standard method, and improved earlier results in the literature.

Proposition 7.1. *(*[KS]*) Let $C_1, \cdots, C_k$ denote the non-identity conjugacy classes of G. Then*

$$||P_H - P_{\{e\}}|| \leq \frac{1}{2} \sum_{i=1}^{k} |C_i \cap H| |C_i|^{-1/2}.$$

We use the perspective of random walk on $Irr(G)$ to prove Proposition 7.2, which is a slight sharpening of Proposition 7.1. (To see that it is sharper, take squares). The usefulness of this sharpening is not yet clear, but note that the random walk viewpoint "explains" the appearance of the quantities $|C_i \cap H||C_i|^{-1}$ in the total variation upper bounds of Propositions 7.1 and 7.2: they are simply the eigenvalues of random walk on $Irr(G)$.

Proposition 7.2. *Let $C_1, \cdots, C_k$ denote the non-identity conjugacy classes of G. Then*

$$||P_H - P_{\{e\}}|| \leq \frac{1}{2} \left[\sum_{i=1}^{k} |C_i \cap H|^2 |C_i|^{-1} \right]^{1/2}.$$

Proof. Note that $P_{\{e\}}$ is simply the Plancherel measure π on $Irr(G)$. Next define η to be the induced representation $Ind_H^G(\hat{1})$, where $\hat{1}$ denotes the trivial representation of H. Then the character of η is real valued, since its value on g is the number of left cosets of H fixed by g. The probability that random walk on $Irr(G)$ defined by η and started at the trivial representation is at ρ after one step is equal to $\frac{d_\rho}{d_\eta} m_\rho(Ind_H^G(\hat{1}))$, where $m_\rho(Ind_H^G(\hat{1}))$ is the multiplicity of ρ in $Ind_H^G(\hat{1})$. Frobenius reciprocity gives that $m_\rho(Ind_H^G(\hat{1}))$ is equal to $\frac{1}{|H|} \sum_{h \in H} \chi^\rho(h)$. Since $d_\eta = \frac{|G|}{|H|}$, it follows that the chance of being at ρ after 1 step of the random walk on $Irr(G)$ is precisely equal to $P_H(\rho)$. Summarizing,

$$||P_H - P_{\{e\}}|| = ||K^1 - \pi||,$$

where K^1 is the distribution on $Irr(G)$ after 1 step started from the trivial representation.

Next, apply part 2 of Lemma 2.1 with $r = 1$ and Lemma 3.1 to conclude that

$$||K^1 - \pi|| \leq \frac{1}{2} \left[\sum_{i=1}^{k} \left(\frac{\chi^{\eta}(C_i)}{d_{\eta}} \right)^2 |C_i| \right]^{1/2}.$$

From the formula for induced characters (page 47 of [Sag]), it follows that $\frac{\chi^{\eta}(C_i)}{d_{\eta}} = \frac{|C_i \cap H|}{|C_i|}$, which completes the proof. □

Acknowledgements

The author was partially supported by NSA grant H98230-05-1-0031 and NSF grant DMS-050391. The author thanks the referee for helpful comments.

References

[Al] Aldous, D., Random walks on finite groups and rapidly mixing Markov chains, in *Séminaire de Probabilités*, XVII, 243-297, LNM 986, Springer, Berlin, 1983.

[An] Andrews, G., *The theory of partitions*, Cambridge University Press, Cambridge, 1984.

[B1] Biane, P., Representations of symmetric groups and free probability, *Adv. Math.* **175** (1997), 126-181.

[B2] Biane, P., Estimation asymptotique des multiplicités dans les puissances tensorielles d'un g-module, *C. R. Acad. Sci. Paris. Sér. I Math.* **316** (1993), 849-852.

[BBO] Biane, P., Bougerol, P., and O'Connell, N., Littelmann paths and Brownian paths, *Duke Math. J.* **130** (2005), 127-167.

[BOO] Borodin, A., Okounkov, A., and Olshanski, G., Asymptotics of Plancherel measure for symmetric groups, *J. Amer. Math. Soc.* **13** (2000), 481-515.

[C] Chatterjee, S., *Concentration inequalities with exchangeable pairs*, Stanford University Ph.D. Thesis, 2005.

[D1] Diaconis, P., *Group representations in probability and statistics*, Institute of Mathematical Statistics, Hayward, CA, 1988.

[D2] Diaconis, P., The cutoff phenomenon in finite Markov chains, *Proc. Nat. Acad. Sci. U.S.A.* **93** (1996), 1659-1664.

[DH] Diaconis, P. and Hanlon, P., Eigen-analysis for some examples of the Metropolis algorithm, in *Hypergeometric functions on domains of positivity, Jack polynomials, and applications*, 99-117, Contemp. Math. 138, 1992.

[DSa] Diaconis, P. and Saloff-Coste, L., Comparison theorems for reversible Markov chains, *Ann. Appl. Probab.* **3** (1993), 696-730.

[DSh] Diaconis, P. and Shahshahani, M., Generating a random permutation with random transpositions, *Z. Wahr. Verw. Gebiete* **57** (1981), 159-179.

[ER] Eymard, P. and Roynette, B., Marches aléatoires sur le dual de SU(2), in *Analyse harmonique sur les groupes de Lie*, 108-152, LNM 497, Springer, Berlin, 1975.

[F1] Fulman, J., Stein's method and Plancherel measure of the symmetric group, *Transac. Amer. Math. Soc.* **357** (2004), 555-570.

[F2] Fulman, J., Stein's method, Jack measure, and the Metropolis algorithm, *J. Combin. Theory Ser. A* **108** (2004), 275-296.

[F3] Fulman, J., Card shuffling and the decomposition of tensor products, *Pacific J. Math* **217** (2004), 247-262.

[F4] Fulman, J., Stein's method and random character ratios, to appear in *Transac. Amer. Math. Soc.*.

[F5] Fulman, J., $GL(n, q)$ and increasing subsequences in non-uniform random permutations, *Annals Combin.* **6** (2002), 19-32.

[F6] Fulman, J., Applications of symmetric functions to cycle and increasing subsequence structure after shuffles, *J. Algebraic Combin.* **16** (2002), 165-194.

[F7] Fulman, J., Separation cutoffs for random walk on irreducible representations, arXiv.org preprint math.PR/0703291 (2007).

[GK] Gnedin, A. and Kerov, S., Derangement characters of the finite general linear group, *Algebr. Represent. Theory* **8** (2005), 255-274.

[GC] Goupil, A. and Chauve, C., Combinatorial operators for Kronecker powers of representations of S_n, *Sém. Lothar. Combin.* **54** (2005/06), Art. B54j, 13 pp. (electronic).

[GM] Grabiner, D. and Magyar, P., Random walks in Weyl chambers and the decomposition of tensor powers, *J. Algebraic Combin.* **2** (1993), 239-260.

[HRT] Hallgren, S., Russell, A., and Ta-Shma, A., Normal subgroup reconstruction and quantum computation using group representations, *Proc. 32nd STOC* (2000), 627-635.

[H] Hildebrand, M., Generating random elements in $SL_n(F_q)$ by random transvections, *J. Algebraic Combin.* **1** (1992), 133-150.

[J] Johansson, K., Discrete orthogonal polynomial ensembles and the Plancherel measure, *Ann. of Math.* **153** (2001), 259-296.

[KS] Kempe, J. and Shalev, A., The hidden subgroup problem and permutation group theory, *Proc. 16th ACM-SIAM SODA* (2005), 1118-1125.

[K] Kuperberg, G., A subexponential-time quantum algorithm for the dihedral hidden subgroup problem, *SIAM J. Comput.* **35** (2005), 170-188.

[L] Lomont, C., The hidden subgroup problem - review and open problems, arXiv.org preprint quant-ph/0411037 (2004).

[Ma] Macdonald, I.G., *Symmetric functions and Hall polynomials*, Second edition, Clarendon Press, Oxford, 1995.

[Mc] McKay, J., Graphs, singularities, and finite groups. The Santa Cruz Conference on Finite Groups (1979), *Proc. Sympos. Pure Math.* **37** (1980), 183-186.

[MR] Moore, C. and Russell, A., On the impossibility of a quantum sieve algorithm for graph isomorphism, arXiv.org preprint quant-ph/0609138, 2006.

[NC] Nielsen, M. and Chuang, I., *Quantum computation and quantum information*, Cambridge University Press, Cambridge, 2000.

[O] Okounkov, A., Random matrices and random permutations, *Internat. Math. Res. Notices* **20** (2000), 1043-1095.

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

[Sag] Sagan, B., *The symmetric group. Representations, combinatorial algorithms, and symmetric functions*, Springer-Verlag, New York, 1991.

[Sal] Saloff-Coste, L., Random walk on finite groups, in *Probability on discrete structures*, 263-346, Encyclopedia Math. Sci. 110, Springer, Berlin, 2004.

[St1] Stanley, R., *Enumerative combinatorics, Vol. 1*, Wadsworth and Brooks/Cole, Monterey, CA, 1986.

[St2] Stanley, R., *Enumerative combinatorics, Vol. 2*, Cambridge Studies in Advanced Mathematics, 62. Cambridge University Press, Cambridge, 1999.

[TZ] Tate, T. and Zelditch, S., Lattice path combinatorics and asymptotics of multiplicities of weights in tensor powers, *J. Funct. Anal.* **217** (2004), 402-447.

[VK] Vershik, A. and Kerov, S., On an infinite dimensional group over a finite field, *Funct. Anal. Appl.* **32** (1999), 147-152.

[Z] Zelevinsky, A., *Representations of finite classical groups: a Hopf algebra approach*, LNM 869, Springer, Berlin, 1981.

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