Statistics and Probability Letters 89 (2014) 77–80

Contents lists available at ScienceDirect

Statistics and Probability Letters

journal homepage: www.elsevier.com/locate/stapro

A random process related to a random walk on upper triangular matrices over a finite field

Martin Hildebrand

Department of Mathematics and Statistics, University at Albany, State University of New York, Albany, NY 12222, United States

ARTICLE INFO

Article history:
Received 27 August 2013
Accepted 1 March 2014
Available online 11 March 2014

Keywords:
Random process
Upper triangular matrices

ABSTRACT

This article considers a random process related to a random walk on n by n upper triangular matrices over a finite field $\mathbb{F}_q$ where q is an odd prime. The walk starts with the identity, and at each step, i is selected at random from $\{2, \ldots, n\}$ and either row i or the negative of row i is added to row $i-1$. This article shows that, for a given q, it takes order n^2 steps for the last column to get close to uniformly distributed over all possibilities for that column.

1. Introduction

A couple of random walks on $U_n(\mathbb{F}_q)$, the group of n by n upper triangular matrices with entries in a finite field $\mathbb{F}_q$ and $n \geq 2$, have been studied. One walk, denoted by $\mathcal{W}_1$, involves at each step adding a times row i to row $i-1$ where i is chosen uniformly from $\{2, \ldots, n\}$ and a is chosen uniformly from $\mathbb{F}_q$. Another walk, denoted by $\mathcal{W}_2$, involves at each step adding ± 1 times row i to row $i-1$ where i chosen uniformly from $\{2, \ldots, n\}$ and each sign is chosen with probability $1/2$. These walks start with the identity matrix, and each step is chosen independent of earlier steps.

In Peres and Sly (2013), they have shown that a lazy version of $\mathcal{W}_1$ is close to uniformly distributed on $U_n(\mathbb{F}_q)$ after order $n^2 \log q$ steps. An important part of their argument involves the last column of the matrix. In Stong (1995), he has shown that after order $n^3 q^2 \log q$ steps, $\mathcal{W}_2$ is close to uniformly distributed on $U_n(\mathbb{F}_q)$.

In this paper, we consider the last column of the matrix in the random walk $\mathcal{W}_2$. We show that if q is a given odd prime, then order n^2 steps suffice to make the last column close to uniformly distributed on all possibilities for the last column. The proof involves representation theory of ${\mathbb{F}_q}^{n-1}$ and the Upper Bound lemma of Diaconis and Shahshahani.

2. Notation and background

Let $\mathbb{F}_q$ be a finite field with q elements in it where q is an odd prime number. Let $U_n(\mathbb{F}_q)$ be the group of n by n upper triangular matrices with 1's on the diagonal, 0's below the diagonal, and entries in $\mathbb{F}_q$ above the diagonal.

If P is a probability on a finite set S and U is the uniform probability on S (i.e. $U(s) = 1/|S|$ for all $s \in S$), then we define the variation distance of P from U by

$$\|P - U\| = \frac{1}{2} \sum_{s \in S} |P(s) - U(s)|.$$

It can be shown that

$$\|P - U\| = \max_{A \subset S} |P(A) - U(A)|$$

where $P(A) = \sum_{s \in A} P(s)$ and the maximum is over all subsets A of S.

E-mail address: mhildebrand@albany.edu.

http://dx.doi.org/10.1016/j.spl.2014.03.001
0167-7152/

If the set S is the set of elements of a finite group G, then the Upper Bound lemma of Diaconis and Shahshahani (described in Diaconis, 1988) can be used to bound $\|P - U\|$.

Lemma 1 (*Upper Bound Lemma of Diaconis and Shahshahani*).

$$\|P - U\|^2 \le \frac{1}{4} \sum_{\rho}^{*} d_\rho \mathrm{Tr}(\hat{P}(\rho)\hat{P}(\rho)^*)$$

where the sum is over all irreducible representations ρ on G up to equivalence, d_ρ is the degree of ρ, the Fourier transform $\hat{P}(\rho) = \sum_{s\in G} P(s)\rho(s)$, the irreducible representations are assumed to be unitary, and $\hat{P}(\rho)^*$ is the conjugate transpose of $\hat{P}(\rho)$.

3. Main result

We shall define random variables $X_0, X_1, X_2, \ldots$ on ${\mathbb{F}_q}^{n-1}$ as follows.

Let X_0 be the column vector with $n-1$ 0's. Let

$$X_{m+1} = A_m X_m + b_m$$

where $(A_0, b_0), (A_1, b_1), \ldots$ are i.i.d. such that

$$P((A_0, b_0) = (M_\ell^+, c_\ell)) = P((A_0, b_0) = (M_\ell^-, -c_\ell)) = \frac{1}{2(n-1)}$$

for $\ell = 2, \ldots, n$, and M_ℓ^+, M_ℓ^-, and c_ℓ are defined as follows. M_n^+ and M_n^- are $(n-1)$ by $(n-1)$ identity matrices. c_n is a column vector with $n-2$ 0's followed by a 1. M_ℓ^+, for $2 \le \ell \le n-1$, is $(n-1)$ by $(n-1)$ matrix with diagonal entries 1, with the entry in position $(\ell-1, \ell)$ being 1, and all other entries 0. M_ℓ^-, for $2 \le \ell \le n-1$, is $(n-1)$ by $(n-1)$ matrix with diagonal entries 1, with the entry in position $(\ell-1, \ell)$ being -1, and with all other entries 0. c_ℓ, for $2 \le \ell \le n-1$, is the zero vector with $n-1$ entries being in one column.

Note that X_m is the last column of the upper triangular matrix after m steps of the random walk $\mathcal{W}_2$. Also note that if $n = 2$, this random process is a simple random walk on $\mathbb{F}_q$.

Let P_m be the probability on ${\mathbb{F}_q}^{n-1}$ such that for all $s \in {\mathbb{F}_q}^{n-1}$, $P_m(s)$ is the probability that $X_m = s$.

The main result is as follows.

Theorem 1. *Suppose q is a given odd prime. Then for some constant $c_q > 0$, if $m > c_q n^2$, then $\|P_m - U\| \to 0$ as $n \to \infty$.*

We assume $n \ge 3$ in the proof.

To prove this theorem, we shall use a recurrence relation involving the Fourier transforms of P_m, and then we use this recurrence relation, some arguments involving discrete probability, and the Upper Bound Lemma.

4. Recurrence relation for Fourier transforms

First observe

$$P(X_{m+1} = j) = \frac{1}{2(n-1)} \sum_{\ell=2}^{n} (P(M_\ell^+ X_m + c_\ell = j) + P(M_\ell^- X_m - c_\ell = j)).$$

For each $k \in {\mathbb{F}_q}^{n-1}$, let $\hat{P}_{m+1}(k)$ denote $\hat{P}_{m+1}(\rho_k)$ where $\rho_k(j) = \omega^{k^T j}$ where $\omega = e^{2\pi i/q}$ and k^T is the transpose of k. Then

$$\begin{aligned}
\hat{P}_{m+1}(k) &= \sum_j P(X_{m+1} = j)\omega^{k^T j} \\
&= \sum_j \frac{1}{2(n-1)} \left(\sum_{\ell=2}^{n} (P(M_\ell^+ X_m + c_\ell = j) + P(M_\ell^- X_m - c_\ell = j)) \right) \omega^{k^T j} \\
&= \sum_{\ell=2}^{n} \frac{1}{2(n-1)} \left(\sum_j P(X_m = (M_\ell^+)^{-1}(j - c_\ell))\omega^{k^T j} + \sum_j P(X_m = (M_\ell^-)^{-1}(j + c_\ell))\omega^{k^T j} \right).
\end{aligned}$$

Note that

$$\begin{aligned}
\sum_j P(X_m = (M_\ell^+)^{-1}(j - c_\ell))\omega^{k^T j} &= \sum_j P(X_m = (M_\ell^+)^{-1} j)\omega^{k^T (j + c_\ell)} \\
&= \sum_j P(X_m = j)\omega^{k^T (M_\ell^+ j + c_\ell)} \\
&= \sum_j P(X_m = j)\omega^{((M_\ell^+)^T k)^T j}\omega^{k^T c_\ell} \\
&= \hat{P}_m((M_\ell^+)^T k)\omega^{k^T c_\ell}.
\end{aligned}$$