

# Random Permutation Matrices

## An Investigation of the Number of Eigenvalues Lying in a Shrinking Interval

Nathaniel Blair-Stahn

September 28, 2005

### **Abstract**

When an  $n \times n$  permutation matrix is chosen at random, each of its  $n$  eigenvalues will lie somewhere on the unit circle. We investigate the average number of these that fall in an arc of the circle that shrinks as the size of the matrix increases, and compare the results against the case where  $n$  points on the circle are chosen independently.

# Contents

<b>1</b>	<b>Introduction</b>	<b>3</b>
<b>2</b>	<b>Background About Permutations and Probability</b>	<b>4</b>
2.1	Cycles and Cycle Structure . . . . .	4
2.2	Probability and Cycle Structure . . . . .	5
<b>3</b>	<b>Permutation Matrices and <math>X_{n,a}</math></b>	<b>6</b>
<b>4</b>	<b>Preliminary Observations</b>	<b>8</b>
4.1	Random Independent Points on the Unit Circle . . . . .	9
4.2	The Number of Eigenvalues at $e^{i\theta}$ . . . . .	9
4.3	Description of $X_{n,a}$ when $a = 0$ and $\ell \leq 1$ . . . . .	10
<b>5</b>	<b>A Technical Lemma</b>	<b>11</b>
<b>6</b>	<b>Calculation of the Limit of <math>E[X_{n,a}]</math> for Rational <math>a</math></b>	<b>13</b>
6.1	The Mean When $a = 0$ . . . . .	14
6.2	The Mean When $a$ Is Rational . . . . .	15
<b>7</b>	<b>Determining the Rate of Convergence of <math>E[X_{n,a}]</math> When <math>a</math> Is Rational</b>	<b>19</b>
7.1	The Error when $a = 0$ . . . . .	20
7.2	The Error for Rational $a$ in General . . . . .	23
7.3	The Total Error Bound . . . . .	28
<b>8</b>	<b>The Mean When <math>a</math> is Irrational</b>	<b>29</b>
8.1	Continued Fractions and Approximation by Rational Numbers . . . . .	30
8.2	Approximating $I_n = (e^{2\pi ia}, e^{2\pi i(a+\ell/n)})$ with a Nearby Interval . . . . .	34
8.3	The Convergence of $E[X_{n,a}]$ for $a \in \mathcal{S}$ . . . . .	40
<b>9</b>	<b>Conclusion</b>	<b>42</b>

# 1 Introduction

A permutation matrix is any  $n \times n$  matrix that has exactly one 1 in each row and column, with all other entries being 0. Here is an example of a  $6 \times 6$  permutation matrix:

$$P = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}$$

All the eigenvalues of a permutation matrix lie on the complex unit circle, and one might wonder how these eigenvalues are distributed when permutation matrices are chosen at random (that is, uniformly from the set of all  $n \times n$  permutation matrices). Some work has already been done in studying the eigenvalues of permutation matrices. Diaconis and Shahshahani [1] looked at the trace (sum of the eigenvalues), and Wieand [7], [6] investigated the number of eigenvalues that lie in a fixed arc of the unit circle. In both cases, the asymptotic behavior for large  $n$  was determined.

Roughly speaking, the number of eigenvalues that lie in a fixed interval on the unit circle will be proportional to the length of the interval and to the dimension  $n$  of the matrix. In this paper, the idea is to allow  $n$  to increase while decreasing the size of the interval, so that the number of eigenvalues lying in it should remain fairly constant on average. In particular, for fixed real numbers  $a \geq 0$  and  $\ell > 0$ , we define the random variable  $X_{n,a}$  to be the number of eigenvalues lying in the “half-open” interval  $I_n = (e^{2\pi ia}, e^{2\pi i(a+\ell/n)}]$  when an  $n \times n$  permutation matrix is chosen at random, and we find the limit of the mean of  $X_{n,a}$  as  $n \rightarrow \infty$ :

## Theorem 1.1

1. Suppose that  $a = p/q$  is a rational number in  $[0, 1)$ , with  $p$  and  $q$  relatively prime.

Then

$$\lim_{n \rightarrow \infty} E[X_{n,a}] = \frac{1}{q} \ln \left( \frac{(q\ell)^{\lfloor q\ell \rfloor}}{\lfloor q\ell \rfloor!} \right).$$

2. For almost every irrational number  $a \in [0, 1)$ ,

$$\lim_{n \rightarrow \infty} E[X_{n,a}] = \ell.$$

The set of irrational numbers to which the second part of this theorem applies will be specified during the proof.

The paper is organized as follows. The next section provides some background about permutations and gives some probabilistic results that will be used later. Section 3 discusses the eigenvalues of permutation matrices and provides a formula for  $X_{n,a}$ . Section 4 draws some comparisons between the distribution of eigenvalues and the distribution of random points on the unit circle. Section 5 provides a technical result that will be used in Section 6 to prove the first part of Theorem 1.1. In Section 7, a rate of convergence is obtained for the limit in part 1 of Theorem 1.1. Finally, part 2 of Theorem 1.1 is proved in Section 8.

## 2 Background About Permutations and Probability

A permutation is any one-to-one mapping of the set  $\{1, 2, \dots, n\}$  onto itself. The set of all permutations of  $n$  elements forms a group under the operation of function composition. This group is known as the symmetric group,  $S_n$ , and it is a simple matter to verify that there are  $n!$  permutations in  $S_n$ . In standard notation, a permutation  $\sigma \in S_n$  is written as

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix},$$

where  $\sigma(1)$  is the image of 1 under  $\sigma$ ,  $\sigma(2)$  is the image of 2, and so on.

### 2.1 Cycles and Cycle Structure

A permutation can also be written in a way that groups together the images of a given number under repeated applications of  $\sigma$ . For example, the permutation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 6 & 4 & 7 & 5 & 9 & 1 & 8 & 2 \end{pmatrix}$$

can be written

$$\sigma = (1\ 3\ 4\ 7)(2\ 6\ 9)(5)(8).$$

The first group of numbers in parentheses indicates that 1 gets mapped to 3, 3 gets mapped to 4, 4 gets mapped to 7, and 7 gets mapped back to 1. Each of the other groupings is interpreted in a similar way. These groups of numbers are called *cycles*, and this notation for permutations is referred to as *cycle notation*. Following are several facts relating to cycles and cycle notation.

- A cycle of  $k$  numbers is referred to as a  $k$ -cycle; for example,  $(1\ 3\ 4\ 7)$  is a 4-cycle.
- A cycle of one number indicates that the number is mapped to itself, and 1-cycles are referred to as *fixed points*. Fixed points are often omitted when writing a permutation in cycle notation.
- If a permutation  $\sigma$  is applied  $k$  times, then the numbers in each  $k$ -cycle in  $\sigma$  will return to their starting positions.
- In general, the *order* of a group element  $g$  is the smallest positive integer  $m$  such that  $g^m$  is the identity. The order of a permutation  $\sigma \in S_n$  is the number of times that  $\sigma$  must be applied in order to return all  $n$  numbers to their starting positions. This will equal the least common multiple of the lengths of all the cycles in  $\sigma$ .
- It does not matter which number is written first in a cycle, as long as the order of the numbers is preserved. For example,  $(1\ 3\ 4\ 7) = (4\ 7\ 1\ 3)$ , but  $(1\ 3\ 4\ 7) \neq (1\ 4\ 3\ 7)$ . Also, the cycles in a permutation can be written in any order. If desired, one can apply any of a number of systematic approaches to keep the notation consistent.

It is useful to define a vector,  $(C_1, C_2, \dots, C_n)$ , called the *cycle structure* of  $\sigma$ , where each entry  $C_k$  gives the number of  $k$ -cycles in  $\sigma$ . Thus, our sample permutation above has a cycle structure of  $(2, 0, 1, 1, 0, 0, 0, 0, 0)$ . Two things to notice about cycle structure are

1. The sum of all the values of  $C_k$  gives the total number of cycles in  $\sigma$ .
2. Since there are  $n$  numbers in  $\sigma$ , the lengths of all the cycles must add up to  $n$ . That is, for  $\sigma \in S_n$ ,

$$\sum_{k=1}^n kC_k = n. \tag{1}$$

## 2.2 Probability and Cycle Structure

At this point, one could ask various questions about cycle structure, such as “How many permutations are there with a given cycle structure?” or, “What is the cycle structure of a ‘typical’ random permutation  $\sigma$ ?” That is, how many fixed points, how many 2-cycles, etc. will  $\sigma$  have, on average?

When the phrase “random permutation” is used in this paper, it means that each permutation in  $S_n$  is equally likely to be chosen. Thus, the probability of picking any one permutation is  $1/n!$ . Using this, the mean, or expected value, of any random variable  $V$  defined on  $S_n$  will be

$$E[V] = \frac{1}{n!} \sum_{\sigma \in S_n} V(\sigma), \quad (2)$$

and the variance of  $V$  will be

$$\text{Var}[V] = \frac{1}{n!} \sum_{\sigma \in S_n} (V(\sigma) - E[V])^2. \quad (3)$$

Notice that the values  $C_1, C_2, \dots, C_n$  for a permutation picked from  $S_n$  are just random variables, and the expectation of these values might provide some insight into the questions posed above. Using standard group theory arguments, it can be shown that the probability of picking a permutation with a particular cycle structure, say  $(t_1, t_2, \dots, t_n)$ , is

$$P(C_1 = t_1, C_2 = t_2, \dots, C_n = t_n) = \begin{cases} \prod_{k=1}^n \frac{1}{k^{t_k} t_k!} & \text{if } \sum_{k=1}^n k t_k = n \\ 0 & \text{otherwise.} \end{cases} \quad (4)$$

This formula can be used to prove a number of facts about the random variables  $C_k$ . The results below are due to Goncharov [3]. (Also see Diaconis and Shahshahani [1].)

$$E[C_k] = \begin{cases} \frac{1}{k} & \text{if } k \leq n \\ 0 & \text{otherwise,} \end{cases} \quad (5)$$

$$E[C_j C_k] = \begin{cases} \frac{1}{jk} & \text{if } j + k \leq n \\ 0 & \text{otherwise} \end{cases} \quad (6)$$

if  $j \neq k$ , and

$$\text{Var}[C_k] = \begin{cases} \frac{1}{k} & \text{if } k \leq n/2 \\ \frac{1}{k} - \frac{1}{k^2} & \text{if } n/2 < k \leq n \\ 0 & \text{otherwise.} \end{cases} \quad (7)$$

### 3 Permutation Matrices and $X_{n,a}$

For each  $\sigma \in S_n$ , let  $M_\sigma$  be the  $n \times n$  matrix constructed by the following rule:

$$(M_\sigma)_{ij} = \begin{cases} 1 & \text{if } j = \sigma(i) \\ 0 & \text{otherwise.} \end{cases} \quad (8)$$

That is, the  $i^{\text{th}}$  row of  $M_\sigma$  has a 1 in the column  $\sigma(i)$  and 0's in all the others. It is easy to verify that  $M_\sigma$  is a permutation matrix (as defined in the introduction), and that this rule in fact defines a one-to-one correspondence between  $S_n$  and the  $n \times n$  permutation matrices. (With  $M_\sigma$  defined in this way, a matrix that is left-multiplied by  $M_\sigma$  will have its rows permuted according to  $\sigma$ , and a matrix that is right-multiplied by  $M_\sigma$  will have its columns permuted according to the inverse of  $\sigma$ .)

Using some elementary facts about  $S_n$  and the properties of determinants, it is not difficult to show that, if  $\sigma$  has cycle structure  $(C_1, C_2, \dots, C_n)$ , then the characteristic polynomial of  $M_\sigma$  is

$$p(\lambda) = \det(M_\sigma - \lambda I) = (-1)^n \prod_{k=1}^n (\lambda^k - 1)^{C_k}, \quad (9)$$

which results because every  $k$ -cycle in  $\sigma$  contributes a factor of  $(-1)^k(\lambda^k - 1)$  to  $p(\lambda)$ . The zeros of  $\pm(\lambda^k - 1)$  are just the  $k^{\text{th}}$  roots of unity, which are  $1, e^{2\pi i/k}, e^{4\pi i/k}, \dots, e^{2(k-1)\pi i/k}$ . (These are just points on the unit circle that are spaced at an angle of  $2\pi/k$  apart.) Since each  $k$ -cycle generates this set of  $k$  eigenvalues, if  $\sigma$  has  $C_k$   $k$ -cycles, then  $M_\sigma$  has  $C_k$  copies of these eigenvalues.

Because of this relationship, the random variable  $X_{n,a}$  can be written in terms of the cycle structure  $(C_1, C_2, \dots, C_n)$ . In order to do this, the following notation will be needed. These definitions will be used extensively in later sections.

**Definition 3.1 (Floor, Ceiling, and Fractional Part)** For all real numbers  $x$ , the largest integer less than or equal to  $x$  is denoted by  $\lfloor x \rfloor$ , read *floor of  $x$* . Similarly, the smallest integer greater than or equal to  $x$  is denoted by  $\lceil x \rceil$ , read *ceiling of  $x$* . In addition, the *fractional part* of  $x$ , written  $\{x\}$ , is defined to be the difference  $x - \lfloor x \rfloor$ . (Notice that  $0 \leq \{x\} < 1$  for all  $x$ .)

Now, consider an arbitrary interval  $I = (e^{2\pi ia}, e^{2\pi ib}]$  on the unit circle, with  $0 < b - a \leq 1$ . For a given  $k$ , we want to determine how many of the eigenvalues corresponding to a  $k$ -cycle will lie in the interval  $I$ . Because of the spacing of the eigenvalues, it is not difficult to see that the interval will contain exactly  $\lfloor kb \rfloor - \lfloor ka \rfloor$  of the  $k$  eigenvalues. Thus, for an arbitrary permutation  $\sigma$ , the number of eigenvalues of  $M_\sigma$  in  $I$  is given by  $\sum_{k=1}^n C_k(\sigma)(\lfloor kb \rfloor - \lfloor ka \rfloor)$ .

To determine the number of eigenvalues of  $M_\sigma$  in  $I_n$ , simply replace  $b$  with  $a + \ell/n$  to obtain

$$X_{n,a}(\sigma) = \sum_{k=1}^n C_k(\sigma) \left( \left\lfloor k \left( a + \frac{\ell}{n} \right) \right\rfloor - \lfloor ka \rfloor \right). \quad (10)$$

The mean of  $X_{n,a}$  is then

$$\begin{aligned} E_{S_n}[X_{n,a}] &= E_{S_n} \left[ \sum_{k=1}^n C_k \left( \left\lfloor k \left( a + \frac{\ell}{n} \right) \right\rfloor - \lfloor ka \rfloor \right) \right] \\ &= \sum_{k=1}^n E_{S_n}[C_k] \left( \left\lfloor k \left( a + \frac{\ell}{n} \right) \right\rfloor - \lfloor ka \rfloor \right) \\ &= \sum_{k=1}^n \frac{1}{k} \left( \left\lfloor k \left( a + \frac{\ell}{n} \right) \right\rfloor - \lfloor ka \rfloor \right). \end{aligned} \quad (11)$$

The restriction that  $b - a \leq 1$  is to ensure that none of the eigenvalues are counted more than once. In the case of  $X_{n,a}$ , this is equivalent to requiring that  $n \geq \ell$ . Thus, equations (10) and (11) are valid for any value of  $\ell > 0$ , provided that  $n$  is large enough. Now, if  $n \leq \ell$ , then  $I_n$  is guaranteed to wrap around the unit circle at least once, and therefore will contain all the eigenvalues of  $M_\sigma$ . That is,  $X_{n,a} = n$  when  $n \leq \ell$ , and from now on, it will be assumed that  $n > \ell$ . Also notice that because the interval lies on a circle, any value of  $a$  greater than 1 corresponds to a value in the range  $[0, 1)$ . From now on, we will assume that  $0 \leq a < 1$ .

## 4 Preliminary Observations

When a permutation is picked with uniform probability from  $S_n$  and the eigenvalues of  $M_\sigma$  are plotted, the result is that  $n$  points on the unit circle have been chosen “at random,” in the sense that the outcome of this experiment is not known beforehand. Obviously, though, not every every point on the circle is equally likely to be picked. In fact, only a finite set of points is possible, and the probability of picking a particular point depends on its location.

Plotting the eigenvalues of a random  $n \times n$  permutation matrix can be compared with plotting  $n$  independent points chosen uniformly from the set of all points on the unit circle. The purpose of this section is to summarize what happens for independent uniform points, and then to make a few quick observations about the eigenvalue distribution of permutation matrices, providing a brief comparison of the two situations.

## 4.1 Random Independent Points on the Unit Circle

In order to provide a basis for comparison, we can define a random variable analogous to  $X_{n,a}$ . Let  $Y_n$  be the number of points that land in the interval  $I_n = (e^{2\pi ia}, e^{2\pi i(a+\ell/n)}]$  when  $n$  independent points are picked according to the uniform distribution.

When the points are picked in this way, there are two intuitive results that follow immediately. First, the distribution of  $Y_n$  should not depend on  $a$ . (Since the points are equally likely to be chosen from anywhere on the circle, the location of the interval should not matter.) Second, the fraction  $Y_n/n$  of points that land in the interval will on average be the same as the ratio of the length of the interval to the circumference of the circle. Thus, by defining  $I_n$  to have a length of  $2\pi\ell/n$ , the mean of  $Y_n$  will have the constant value  $\ell$ , regardless of the value of  $n$ .

These results also become apparent by noticing that  $Y_n$  is a binomial random variable, as follows. If a single point on the unit circle is chosen at random (uniformly), the probability that it will lie in  $I_n$  is  $p = \ell/n$ . When  $n$  points are chosen independently, the number of points  $Y_n$  lying in  $I_n$  will, by definition, be binomial with parameters  $(n, \ell/n)$ . Binomial random variables are standard in probability, and the mean and variance in this case are known to be

$$E[Y_n] = n \binom{\ell}{n} = \ell, \quad (12)$$

and

$$\text{Var}[Y_n] = n \binom{\ell}{n} \left(1 - \frac{\ell}{n}\right) = \ell \left(1 - \frac{\ell}{n}\right). \quad (13)$$

In fact, as  $n \rightarrow \infty$ ,  $Y_n$  converges in distribution to a Poisson random variable with parameter  $\ell$ .

## 4.2 The Number of Eigenvalues at $e^{i\theta}$

When points on the unit circle are chosen at random under the uniform distribution, the probability of picking any particular point  $e^{i\theta}$  is 0. The eigenvalues of permutation matrices, however, occur only at certain values of  $\theta$ , so the probability of choosing one of these points is positive, while the probability for any other point is 0.

In order to gain some insight into this problem, define a random variable  $Z_{n,\theta}$  to be the number of eigenvalues of  $\sigma \in S_n$  equal to  $e^{i\theta}$ . The variable  $Z_{n,\theta}$  is already well understood;

see, for example, [3], [5]. Presented here is a brief explanation of what happens to the mean of  $Z_{n,\theta}$  as  $n \rightarrow \infty$ .

First consider the case when  $\theta = 0$ . Every cycle in a permutation  $\sigma$  produces the eigenvalue 1, so the number of eigenvalues at  $\theta = 0$  will equal the total number of cycles in  $\sigma$ . Recall that the number of cycles in  $\sigma$  is the sum of all the values of  $C_k$  in the cycle structure. Thus,

$$Z_{n,0} = \sum_{k=1}^n C_k, \quad (14)$$

and the mean of  $Z_{n,0}$  is

$$E[Z_{n,0}] = \sum_{k=1}^n E[C_k] = \sum_{k=1}^n \frac{1}{k}. \quad (15)$$

For large  $n$ , this sum can be approximated by  $\ln n$ , resulting in

$$E[Z_{n,0}] = \ln n + O(1). \quad (16)$$

In general, if  $\theta = 2\pi p/q$  with  $p$  and  $q$  relatively prime, then a  $k$ -cycle contributes one eigenvalue if  $k$  divides  $q$ . An argument similar to the one above shows that in this case

$$E[Z_{n,\theta}] = \frac{1}{q} \ln n + O(1). \quad (17)$$

(An explicit derivation of this result can be found in the proof of Lemma 8.13.) If  $\theta$  is an irrational multiple of  $2\pi$ , then no eigenvalues can occur there, so  $Z_{n,\theta} = 0$  for all  $n$  in this case. This behavior is quite different from the uniform case.

### 4.3 Description of $X_{n,a}$ when $a = 0$ and $\ell \leq 1$

This is a special case for which very little calculation is involved in determining the behavior of  $X_{n,a}$ . With  $a = 0$ , the interval  $I_n$  starts at 0 and ends at  $2\pi\ell/n$ , and equation (10) simplifies to

$$X_{n,0} = \sum_{k=1}^n C_k \left\lfloor \frac{k\ell}{n} \right\rfloor. \quad (18)$$

Since the largest cycle that can occur in  $\sigma$  is an  $n$ -cycle, the first position on the unit circle where an eigenvalue can occur is at an angle of  $\theta = 2\pi/n$ . If  $\ell < 1$ , then  $X_{n,0} = 0$  because the interval ends before reaching the first possible eigenvalue. This can also be seen from (18) by noting that  $\lfloor k\ell/n \rfloor = 0$  for all  $k \leq n$  if  $\ell < 1$ .

Now if  $\ell = 1$ , then the interval ends exactly where the first eigenvalue can occur, so we have

$$X_{n,0} = \begin{cases} 1 & \text{if } \sigma \text{ has an } n\text{-cycle} \\ 0 & \text{otherwise.} \end{cases}$$

The probability that  $\sigma$  has an  $n$ -cycle is  $1/n$ , so in this case  $X_{n,0}$  is just a Bernoulli random variable with parameter  $1/n$ , and we have

$$E[X_{n,0}] = \frac{1}{n} \tag{19}$$

and

$$\text{Var}[X_{n,0}] = \frac{1}{n} \left(1 - \frac{1}{n}\right) = \frac{n-1}{n^2}. \tag{20}$$

Both the mean and the variance approach 0 as  $n \rightarrow \infty$ .

**Remark.** A similar analysis shows that an analogous ‘gap’ occurs around each rational point  $a$ ; in particular, if  $a = p/q$  in lowest terms, then no eigenvalues can fall in the interval  $I_n$  if  $\ell < 1/q$ . For irrational values of  $a$ , this sort of gap does not occur. No matter how small  $\ell$  is, there will always be some values of  $n$  that produce eigenvalues in the interval  $I_n$ .

These results illuminate some of the differences between the distribution of eigenvalues and that of independent points on the circle. When  $n$  is small, it is easy to calculate the value of  $X_{n,a}$ , and of  $E[X_{n,a}]$  or other quantities describing the distribution of eigenvalues. As  $n$  increases, however, exact results require more and more computation, and it is more useful to try to find general trends that will provide a picture of what is happening. One might expect that as  $n$  gets larger, the non-uniformity in the distribution of eigenvalues would tend to even out, and the situation might start looking more like the uniform case. The motivation for looking at the large  $n$  limit of  $E[X_{n,a}]$  is to investigate the extent to which this idea provides an accurate description.

## 5 A Technical Lemma

This section contains some elementary results that will be needed throughout the rest of the paper. We begin with a definition that will be used in Section 7.

**Definition 5.1 (The Harmonic Series)** Define  $H_0 = 0$ , and for each positive integer  $m$ , define

$$H_m = \sum_{k=1}^m \frac{1}{k}.$$

This well-known sum grows logarithmically as  $m$  increases. This sum and other similar ones arise in the calculation of the large  $n$  limit of  $E[X_{n,a}]$ . The following lemma gives a precise result about approximating such sums with logarithms. The lemma and the corollary immediately succeeding it will be the main tools used to prove the theorems in the next two sections.

**Lemma 5.2** 1. Let  $x$  and  $y$  be integers with  $1 \leq x \leq y$ . Then

$$\sum_{k=x}^y \frac{1}{k} = \ln\left(\frac{y}{x}\right) + \epsilon_0(x, y),$$

where

$$\frac{1}{2} \left( \frac{1}{x} + \frac{1}{y} \right) \leq \epsilon_0(x, y) \leq \frac{1}{x}.$$

2. Let  $x$  and  $y$  be non-negative integers, with  $x \leq y$ . Then for any fixed positive number  $u$ ,

$$\sum_{k=x}^y \frac{1}{k+u} = \ln\left(\frac{y+u}{x+u}\right) + \epsilon_u(x, y),$$

where

$$\frac{1}{2} \left( \frac{1}{x+u} + \frac{1}{y+u} \right) \leq \epsilon_u(x, y) \leq \frac{1}{x+u}.$$

**Proof.** Observe that for any integers  $0 \leq x \leq y$  and any  $u > 0$ , comparing the sum in part 2 with the integral  $\int_x^y \frac{1}{t+u} dt$  shows that

$$\sum_{k=x}^y \frac{1}{k+u} = \frac{1}{x+u} + \ln(y+u) - \ln(x+u) - \delta_u(x, y),$$

where

$$0 \leq \delta_u(x, y) \leq \frac{1}{2} \left( \frac{1}{y+u} - \frac{1}{x+u} \right).$$

Part 2 follows by setting  $\epsilon_u(x, y) = 1/(x+u) - \delta_u(x, y)$ . If  $x > 0$ , the same proof works for  $u = 0$ , resulting in part 1.  $\square$

**Remark.** Part 1 of Lemma 5.2 shows that  $\ln(m) + 1/2 \leq H_m \leq \ln(m) + 1$  for all  $m \geq 1$ .

**Corollary 5.3** Let  $\alpha > 0$  and  $\beta \geq 0$ , and suppose  $(L_n)$  and  $(M_n)$  are sequences of integers which satisfy

$$\frac{L_n}{n} \rightarrow L > 0$$

and

$$\frac{M_n}{n} \rightarrow M \geq L.$$

Then

$$\lim_{n \rightarrow \infty} \sum_{k=L_n}^{M_n} \frac{1}{\alpha k + \beta} = \frac{1}{\alpha} \ln \left( \frac{M}{L} \right).$$

**Proof.** The conditions on  $(L_n)$  and  $(M_n)$  imply that  $0 < L_n \leq M_n$  for large enough  $n$ . Thus, we can apply either part 1 or part 2 of Lemma 5.2 to obtain

$$\sum_{k=L_n}^{M_n} \frac{1}{\alpha k + \beta} = \frac{1}{\alpha} \ln \left( \frac{M_n + u}{L_n + u} \right) + \frac{1}{\alpha} \epsilon_u(L_n, M_n), \quad (21)$$

where  $u = \beta/\alpha$ . Because the sequences  $(L_n)$  and  $(M_n)$  must diverge to  $\infty$ , the quantity  $\epsilon_u(L_n, M_n)$  goes to zero as  $n \rightarrow \infty$ , and clearly

$$\frac{1}{\alpha} \ln \left( \frac{M_n + u}{L_n + u} \right) \rightarrow \frac{1}{\alpha} \ln \left( \frac{M}{L} \right). \quad \square \quad (22)$$

## 6 Calculation of the Limit of $E[X_{n,a}]$ for Rational $a$

This section is devoted to finding the limit of the mean of  $X_{n,a}$  when  $a$  is rational. The following theorem is a restatement of part 1 of Theorem 1.1.

**Theorem 6.1** If  $a=0$ , then

$$\lim_{n \rightarrow \infty} E[X_{n,a}] = \ln \left( \frac{\ell^{[\ell]}}{[\ell]!} \right),$$

and if  $a = p/q$  with  $p$  and  $q$  relatively prime (and  $q > 0$ ), then

$$\lim_{n \rightarrow \infty} E[X_{n,a}] = \frac{1}{q} \ln \left( \frac{(q\ell)^{[q\ell]}}{[q\ell]!} \right).$$

As the statement of the theorem suggests, the proof will be divided into two parts. In Section 6.1, the result is proved first for the case when  $a = 0$ , then is extended to include any rational  $a$  in Section 6.2. Although the proof splits naturally in this way, the formula for  $a = 0$  actually corresponds to  $q = 1$  in the more general case.

### 6.1 The Mean When $a = 0$

In the case where  $a = 0$  and  $I_n = (1, e^{2\pi i \ell/n}]$ , equations (10) and (11) have a particularly simple form:

$$X_{n,0} = \sum_{k=1}^n C_k \left\lfloor \frac{k\ell}{n} \right\rfloor, \quad (23)$$

and

$$E[X_{n,0}] = \sum_{k=1}^n \frac{1}{k} \left\lfloor \frac{k\ell}{n} \right\rfloor. \quad (24)$$

Observe that  $\lfloor k\ell/n \rfloor$  takes on only integer values, specifically all integers from 0 to  $\lfloor \ell \rfloor$ . Thus, it might be useful to group the terms in the sum according to this value. For this purpose, denote the value of  $\lfloor k\ell/n \rfloor$  by  $j$ . We will group the terms by determining which values of  $k$  correspond to a given value of  $j$ , then adding up the groups for each  $j$ . Now, if  $\lfloor k\ell/n \rfloor = j$ , then  $j \leq \frac{k\ell}{n} < j+1$ , or  $j\frac{n}{\ell} \leq k < (j+1)\frac{n}{\ell}$ . The first group of terms, when  $j = 0$ , does not contribute to the sum. For the last group, when  $j = \lfloor \ell \rfloor$ , the upper limit on  $k$  is  $n$  rather than  $(\lfloor \ell \rfloor + 1)\frac{n}{\ell}$ , so this group will be written separately from the others. Grouping the terms in this way results in

$$E[X_{n,0}] = \sum_{j=1}^{\lfloor \ell \rfloor - 1} \sum_{k=\lceil j\frac{n}{\ell} \rceil}^{\lceil (j+1)\frac{n}{\ell} \rceil - 1} \frac{j}{k} + \sum_{k=\lceil \lfloor \ell \rfloor \frac{n}{\ell} \rceil}^n \frac{\lfloor \ell \rfloor}{k}, \quad (25)$$

where the limits on  $k$  are a direct result of the above inequalities and the fact that  $k$  must be an integer.

The sums in  $k$  are of the form in Corollary 5.3, with  $\alpha = 1/j$  and  $\beta = 0$ . In order to find the limit of these sums using the lemma, the following results are needed:

$$\lim_{n \rightarrow \infty} \frac{\lceil j\frac{n}{\ell} \rceil}{n} = \frac{j}{\ell}; \quad (26)$$

$$\lim_{n \rightarrow \infty} \frac{\lceil (j+1)\frac{n}{\ell} \rceil - 1}{n} = \frac{j+1}{\ell}; \quad (27)$$

$$\lim_{n \rightarrow \infty} \frac{\lceil \lfloor \ell \rfloor \frac{n}{\ell} \rceil}{n} = \frac{\lfloor \ell \rfloor}{\ell}. \quad (28)$$

These limits are easily attained by noting that, for all real  $x$ ,  $\lceil x \rceil = x + \varepsilon_x$ , where  $0 \leq \varepsilon_x < 1$ . Applying the lemma then gives

$$\lim_{n \rightarrow \infty} E[X_{n,0}] = \sum_{j=1}^{\lfloor \ell \rfloor - 1} j \ln \left( \frac{j+1}{j} \right) + \lfloor \ell \rfloor \ln \left( \frac{\ell}{\lfloor \ell \rfloor} \right) \quad (29)$$

$$= \ln \left( \prod_{j=1}^{\lfloor \ell \rfloor - 1} \frac{(j+1)^j}{j^j} \right) + \ln \left( \frac{\ell^{\lfloor \ell \rfloor}}{\lfloor \ell \rfloor^{\lfloor \ell \rfloor}} \right) \quad (30)$$

$$= \ln \left( \frac{\lfloor \ell \rfloor^{\lfloor \ell \rfloor - 1}}{(\lfloor \ell \rfloor - 1)!} \right) + \ln \left( \frac{\ell^{\lfloor \ell \rfloor}}{\lfloor \ell \rfloor^{\lfloor \ell \rfloor}} \right) \quad (31)$$

$$= \ln \left( \frac{\ell^{\lfloor \ell \rfloor}}{\lfloor \ell \rfloor!} \right), \quad (32)$$

which proves the first part of Theorem 6.1.

## 6.2 The Mean When $a$ Is Rational

Now we no longer assume  $a$  to be 0 and return to equation (10) for  $X_{n,a}$ :

$$X_{n,a} = \sum_{k=1}^n C_k \left( \left\lfloor ka + \frac{k\ell}{n} \right\rfloor - \lfloor ka \rfloor \right). \quad (33)$$

A little thought shows that in general,

$$\lceil x + y \rceil = \begin{cases} \lfloor x \rfloor + \lfloor y \rfloor & \text{if } \{x\} + \{y\} < 1 \\ \lfloor x \rfloor + \lfloor y \rfloor + 1 & \text{otherwise} \end{cases} \quad (34)$$

for any real numbers  $x$  and  $y$ . Applying (34) to the first term in (33) gives

$$\left\lfloor ka + \frac{k\ell}{n} \right\rfloor = \begin{cases} \lfloor ka \rfloor + \lfloor k\ell/n \rfloor & \text{if } \{ka\} + \left\{ \frac{k\ell}{n} \right\} < 1 \\ \lfloor ka \rfloor + \lfloor k\ell/n \rfloor + 1 & \text{otherwise,} \end{cases} \quad (35)$$

and so

$$X_{n,a} = \sum_{k=1}^n C_k \left( \left\lfloor ka + \frac{k\ell}{n} \right\rfloor - \lfloor ka \rfloor \right) \quad (36)$$

$$= \sum_{k=1}^n C_k \left\lfloor \frac{k\ell}{n} \right\rfloor + \sum_{\substack{k: \{ka\} + \left\{ \frac{k\ell}{n} \right\} \geq 1, \\ 1 \leq k \leq n}} C_k. \quad (37)$$

Thus, the number of eigenvalues  $X_{n,a}$  in the interval  $(e^{2\pi ia}, e^{2\pi i(a+\ell/n)})$  equals the number of eigenvalues  $X_{n,0}$  in the interval  $(1, e^{2\pi i\ell/n}]$ , plus  $\sum C_k$  for values of  $k$  such that

$\{ka\} + \left\{\frac{k\ell}{n}\right\} \geq 1$ . Taking the expected value gives

$$E[X_{n,a}] = \sum_{k=1}^n \frac{1}{k} \left\lfloor \frac{k\ell}{n} \right\rfloor + \sum_{\substack{k: \{ka\} + \left\{\frac{k\ell}{n}\right\} \geq 1, \\ 1 \leq k \leq n}} \frac{1}{k} \quad (38)$$

$$= E[X_{n,0}] + V_n, \quad (39)$$

where  $V_n$  denotes the second sum in (38). Now the problem is to find the limit of  $V_n$ , which will require determining the values of  $k$  for which  $\{ka\} + \left\{\frac{k\ell}{n}\right\} \geq 1$ .

Here, we turn our attention to the case when  $a$  is rational. Let  $a = p/q$  with  $p$  and  $q$  relatively prime (and  $q > 0$ ). Then  $\{ka\} = \left\{\frac{kp}{q}\right\}$  takes on only a finite number of values, namely all fractions of the form  $x/q$ , where  $x$  is an integer between 0 and  $q-1$  (inclusive). Although the order of the  $x$ 's depends on  $p$ , observe that the sequence  $x/q$  repeats with a period of  $q$  as  $k$  increases. This suggests that it may be helpful to group the terms in  $V_n$  according to the value of  $\left\{\frac{kp}{q}\right\}$ .

First we define a new index  $i$  whose values will correspond to each of the  $q$  possible values of  $\left\{\frac{kp}{q}\right\}$ . For each integer  $i = 1, 2, \dots, q$ , let  $w_i$  be the number between 0 and  $q-1$  such that  $\left\{\frac{w_i p}{q}\right\} = 1 - \frac{i}{q}$ . Since the sequence  $\left\{\frac{kp}{q}\right\}$  repeats, whenever  $k \equiv w_i \pmod{q}$ , the value of  $\left\{\frac{kp}{q}\right\}$  will be  $1 - \frac{i}{q}$ . Thus, for such  $k$ , the condition  $\left\{\frac{kp}{q}\right\} + \left\{\frac{k\ell}{n}\right\} \geq 1$  becomes  $\left\{\frac{k\ell}{n}\right\} \geq \frac{i}{q}$ . Notice that if  $i = q$  (corresponding to  $k \equiv 0 \pmod{q}$ ), this condition becomes  $\left\{\frac{k\ell}{n}\right\} \geq 1$ . Since the fractional part is always less than one, this can never occur, and so the case  $i = q$  can be omitted from the sum.

Now, for each value of  $i$  from 1 to  $q-1$ , it needs to be determined which  $k$  satisfy  $\left\{\frac{k\ell}{n}\right\} \geq \frac{i}{q}$ . Between each pair of consecutive integers from 0 to  $\lceil \ell \rceil$ , there is a (possibly empty) set of values of the form  $k\ell/n$  that satisfy this condition. In particular, the fractional part of  $k\ell/n$  is in the correct range iff one of the following pairs of inequalities holds:

$$\frac{i}{q} \leq \frac{k\ell}{n} < 1, 1 + \frac{i}{q} \leq \frac{k\ell}{n} < 2, \dots, \lfloor \ell \rfloor - 1 + \frac{i}{q} \leq \frac{k\ell}{n} < \lfloor \ell \rfloor, \lfloor \ell \rfloor + \frac{i}{q} \leq \frac{k\ell}{n} \leq \ell.$$

These inequalities translate directly into bounds on  $k$ , and thus each pair of inequalities identifies a set of values of  $k$  that will contribute to the sum for a particular  $i$ . We will use a third index,  $j$ , to identify these groups of terms. Except for the last group, the general limits on  $k$  are  $(j + \frac{i}{q})\frac{n}{\ell} \leq k < (j+1)\frac{n}{\ell}$ , where  $j$  ranges from 0 to  $\lfloor \ell \rfloor - 1$ .

In the last group of terms (corresponding to  $j = \lfloor \ell \rfloor$ ), the upper limit on  $k$  is simply  $n$ . Notice also that this group is only present if  $\lfloor \ell \rfloor + \frac{i}{q} \leq \ell$ , or  $\frac{i}{q} \leq \{\ell\}$ . Because of this, the

limits on  $i$  as well as  $k$  are different for the last group. The value of  $i$ , instead of ranging over all the integers from 1 to  $q - 1$ , only reaches the largest integer that is less than or equal to  $q\{\ell\}$ . That is, the limits on  $i$  will be  $1 \leq i \leq \lfloor q\{\ell\} \rfloor$ , which can be rewritten as  $1 \leq i \leq \lfloor q\ell \rfloor - q\lfloor \ell \rfloor$ .

Using these limits to group the terms in the sum, and keeping in mind that for each  $i$  we only count values of  $k$  such that  $k \equiv w_i \pmod{q}$ , we arrive at the following form for  $V_n$  when  $a$  is rational:

$$V_n = \sum_{i=1}^{q-1} \sum_{j=0}^{\lfloor \ell \rfloor - 1} \sum_{\substack{k=\lfloor (j+\frac{i}{q})\frac{n}{\ell} \rfloor \\ k \equiv w_i \pmod{q}}}^{\lfloor (j+1)\frac{n}{\ell} \rfloor - 1} \frac{1}{k} + \sum_{i=1}^{\lfloor q\ell \rfloor - q\lfloor \ell \rfloor} \sum_{\substack{k=\lfloor (\lfloor \ell \rfloor + \frac{i}{q})\frac{n}{\ell} \rfloor \\ k \equiv w_i \pmod{q}}}^n \frac{1}{k}. \quad (40)$$

Now, every  $k$  for which  $k \equiv w_i \pmod{q}$  can be written as  $k = qk' + w_i$ , for some integer  $k'$ . Making this substitution, the sum becomes

$$V_n = \sum_{i=1}^{q-1} \sum_{j=0}^{\lfloor \ell \rfloor - 1} \sum_{k'=L_{n,ij}}^{M_{n,ij}} \frac{1}{qk' + w_i} + \sum_{i=1}^{\lfloor q\ell \rfloor - q\lfloor \ell \rfloor} \sum_{k'=L'_{n,i}}^{M'_{n,i}} \frac{1}{qk' + w_i}, \quad (41)$$

where

$$L_{n,ij} = \left\lfloor \frac{1}{q} \left( \left\lfloor \left( j + \frac{i}{q} \right) \frac{n}{\ell} \right\rfloor - w_i \right) \right\rfloor, \quad (42)$$

$$M_{n,ij} = \left\lfloor \frac{1}{q} \left( \left\lfloor (j+1)\frac{n}{\ell} \right\rfloor - 1 - w_i \right) \right\rfloor, \quad (43)$$

$$L'_{n,i} = \left\lfloor \frac{1}{q} \left( \left\lfloor \left( \lfloor \ell \rfloor + \frac{i}{q} \right) \frac{n}{\ell} \right\rfloor - w_i \right) \right\rfloor, \quad (44)$$

$$M'_{n,i} = \left\lfloor \frac{1}{q} (n - w_i) \right\rfloor. \quad (45)$$

Here, the sums in  $k'$  have the form in Corollary 5.3, this time with  $\alpha = q$  and  $\beta = w_i$ . The relevant limits in this case are

$$\lim_{n \rightarrow \infty} \frac{L_{n,ij}}{n} = \frac{1}{q\ell} \left( j + \frac{i}{q} \right), \quad (46)$$

$$\lim_{n \rightarrow \infty} \frac{M_{n,ij}}{n} = \frac{1}{q\ell} (j+1), \quad (47)$$

$$\lim_{n \rightarrow \infty} \frac{L'_{n,i}}{n} = \frac{1}{q\ell} \left( \lfloor \ell \rfloor + \frac{i}{q} \right), \quad (48)$$

$$\lim_{n \rightarrow \infty} \frac{M'_{n,i}}{n} = \frac{1}{q}. \quad (49)$$

Notice that the  $w_i$  do not appear in the above limits, indicating that these limits do not depend on the value of  $p$ . Hence, all dependence on  $p$  disappears when we apply Corollary 5.3, which gives

$$\lim_{n \rightarrow \infty} V_n = \sum_{i=1}^{q-1} \sum_{j=0}^{\lfloor \ell \rfloor - 1} \frac{1}{q} \ln \left( \frac{j+1}{j + \frac{i}{q}} \right) + \sum_{i=1}^{\lfloor q\ell \rfloor - q\lfloor \ell \rfloor} \frac{1}{q} \ln \left( \frac{\ell}{\lfloor \ell \rfloor + \frac{i}{q}} \right) \quad (50)$$

$$= \frac{1}{q} \ln \left( \prod_{i=1}^{q-1} \prod_{j=0}^{\lfloor \ell \rfloor - 1} \frac{q(j+1)}{qj+i} \right) + \frac{1}{q} \ln \left( \prod_{i=1}^{\lfloor q\ell \rfloor - q\lfloor \ell \rfloor} \frac{q\ell}{q\lfloor \ell \rfloor + i} \right) \quad (51)$$

$$= \frac{1}{q} \ln \left( \frac{(q^{\lfloor \ell \rfloor} \lfloor \ell \rfloor!)^{(q-1)}}{\prod_{i=1}^{q-1} \prod_{j=0}^{\lfloor \ell \rfloor - 1} (qj+i)} \right) + \frac{1}{q} \ln \left( \frac{(q\ell)^{(\lfloor q\ell \rfloor - q\lfloor \ell \rfloor)}}{\prod_{i=1}^{\lfloor q\ell \rfloor - q\lfloor \ell \rfloor} (q\lfloor \ell \rfloor + i)} \right) \quad (52)$$

$$= \frac{1}{q} \ln \left( \frac{(q^{\lfloor \ell \rfloor} \lfloor \ell \rfloor!)^q}{(q\lfloor \ell \rfloor)!} \right) + \frac{1}{q} \ln \left( \frac{(q\ell)^{\lfloor q\ell \rfloor} (q\lfloor \ell \rfloor)!}{(q\ell)^{q\lfloor \ell \rfloor} \lfloor q\ell \rfloor!} \right). \quad (53)$$

The last step follows from expanding the two products in the denominators. This shows that  $\prod_{i=1}^{q-1} \prod_{j=0}^{\lfloor \ell \rfloor - 1} (qj+i)$  is just the product of all the numbers from 1 to  $q\lfloor \ell \rfloor$ , excluding multiples of  $q$ . Thus

$$\prod_{i=1}^{q-1} \prod_{j=0}^{\lfloor \ell \rfloor - 1} (qj+i) = \frac{\prod_{i'=1}^{q\lfloor \ell \rfloor} i'}{\prod_{j'=1}^{\lfloor \ell \rfloor} qj'} = \frac{(q\lfloor \ell \rfloor)!}{q^{\lfloor \ell \rfloor} \lfloor \ell \rfloor!}. \quad (54)$$

In addition,  $\prod_{i=1}^{\lfloor q\ell \rfloor - q\lfloor \ell \rfloor} (q\lfloor \ell \rfloor + i)$  is the product of all the numbers from  $q\lfloor \ell \rfloor + 1$  to  $\lfloor q\ell \rfloor$ , which is just  $\frac{\lfloor q\ell \rfloor!}{(q\lfloor \ell \rfloor)!}$ .

When the arguments of the two logarithms in (53) are multiplied, some of the terms cancel out, resulting in

$$\lim_{n \rightarrow \infty} V_n = \frac{1}{q} \ln \left[ \left( \frac{\lfloor \ell \rfloor!}{\ell^{\lfloor \ell \rfloor}} \right)^q \left( \frac{(q\ell)^{\lfloor q\ell \rfloor}}{\lfloor q\ell \rfloor!} \right) \right] \quad (55)$$

$$= \ln \left( \frac{\lfloor \ell \rfloor!}{\ell^{\lfloor \ell \rfloor}} \right) + \frac{1}{q} \ln \left( \frac{(q\ell)^{\lfloor q\ell \rfloor}}{\lfloor q\ell \rfloor!} \right). \quad (56)$$

Adding equations (32) and (56) yields

$$\lim_{n \rightarrow \infty} E \left[ X_{n, \frac{p}{q}} \right] = \frac{1}{q} \ln \left( \frac{(q\ell)^{\lfloor q\ell \rfloor}}{\lfloor q\ell \rfloor!} \right). \quad (57)$$

Thus Theorem 6.1 (and hence the first part of Theorem 1.1) has been proved.  $\square$

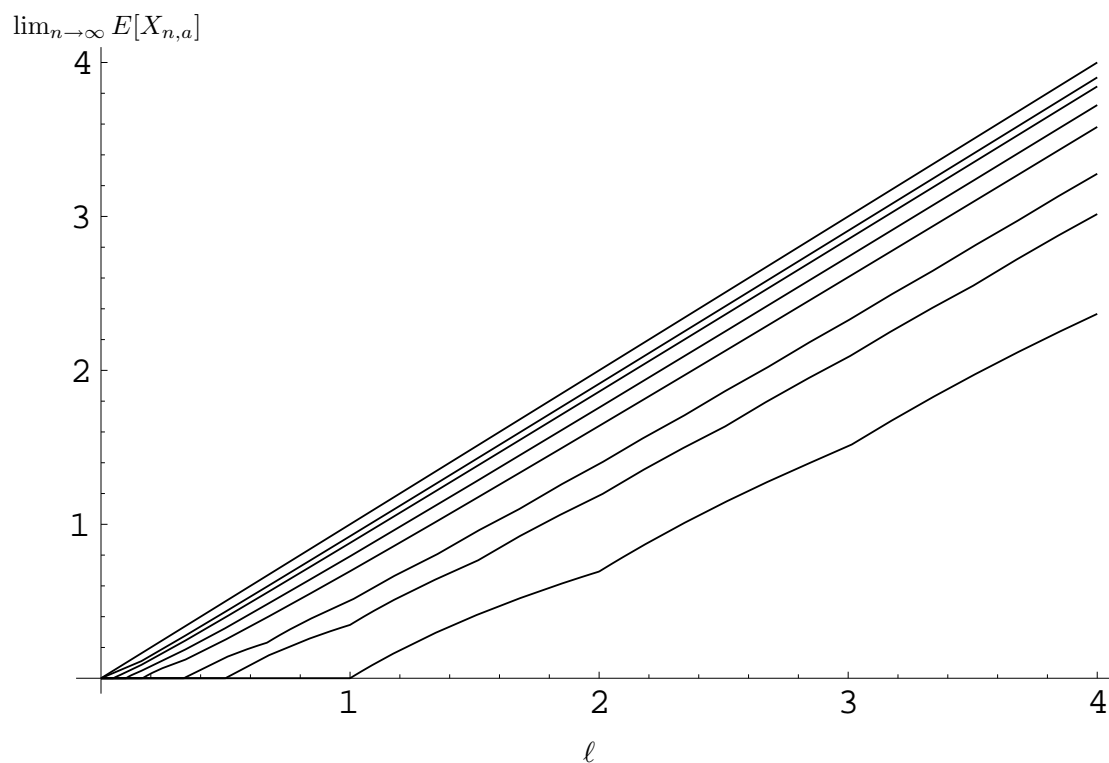


Figure 1: The curves above show  $\lim_{n \rightarrow \infty} E[X_{n,a}]$  as a function of  $\ell$  for various values of  $a$ . The top curve is the line  $f(\ell) = \ell$ . The other curves, from the bottom, are  $\lim_{n \rightarrow \infty} E[X_{n,a}]$  for  $a = 0$ ,  $a = \frac{1}{2}$ ,  $a = \frac{1}{3}$ ,  $a = \frac{1}{6}$ ,  $a = \frac{1}{10}$ ,  $a = \frac{1}{20}$ , and  $a = \frac{1}{35}$ .

We can make a few simple observations about the limit (57). First, note that the limiting function depends only on  $q$ , so for rational  $a$  the limit is a function only of the denominator. Figure 1 shows  $\lim_{n \rightarrow \infty} E[X_{n,a}]$  as a function of  $\ell$  for various values of  $a$ . Based on the curves in the figure, as  $q$  increases, the limit function appears to increase, possibly towards the line  $f(\ell) = \ell$ . If we think of the irrational  $a$  case as a limit of large  $q$ , this observation gives some feeling for the relationship between the two parts of Theorem 1.1. This idea will be explored carefully in Section 8.

## 7 Determining the Rate of Convergence of $E[X_{n,a}]$ When $a$ Is Rational

In this section, we will look at the rate of convergence of  $E[X_{n,a}]$  when  $a$  is rational. The error bound derived in this section will be needed in Section 8 to prove the second part of

Theorem 1.1. To begin, we introduce a new variable to represent the difference between  $E[X_{n,a}]$  and the limit found in Section 6. For a rational number  $a = p/q$ , let

$$A_{n,a} = \frac{1}{q} \ln \left( \frac{(q\ell)^{\lfloor q\ell \rfloor}}{\lfloor q\ell \rfloor!} \right) - E \left[ X_{n, \frac{p}{q}} \right].$$

The goal will be to bound the quantity  $A_{n,a}$  using Lemma 5.2. Using equations (39) and (56), the error  $A_{n,a}$  can be expressed as the sum of  $A_{n,0}$  and a remainder term, which we will call  $A'_{n,a}$ :

$$\begin{aligned} A_{n,a} &= \left[ \ln \left( \frac{\ell^{\lfloor \ell \rfloor}}{\lfloor \ell \rfloor!} \right) - E[X_{n,0}] \right] + \left[ \lim_{n \rightarrow \infty} V_n(a, \ell) - V_n(a, \ell) \right] \\ &= A_{n,0} + A'_{n,a}, \end{aligned} \tag{58}$$

The values of  $A_{n,0}$  and  $A'_{n,a}$  will be estimated separately.

### 7.1 The Error when $a = 0$

From equation (25), we have

$$A_{n,0} = \ln \left( \frac{\ell^{\lfloor \ell \rfloor}}{\lfloor \ell \rfloor!} \right) - \left[ \sum_{j=1}^{\lfloor \ell \rfloor - 1} \sum_{k=\lceil j \frac{n}{\ell} \rceil}^{\lceil (j+1) \frac{n}{\ell} \rceil - 1} \frac{j}{k} + \sum_{k=\lceil \lfloor \ell \rfloor \frac{n}{\ell} \rceil}^n \frac{\lfloor \ell \rfloor}{k} \right]. \tag{59}$$

Now Lemma 5.2 can be applied to the sums in  $k$ . To simplify the notation in this step, let

$$\varepsilon_j = \varepsilon_0 \left( \lceil j \frac{n}{\ell} \rceil, \lceil (j+1) \frac{n}{\ell} \rceil - 1 \right),$$

for  $0 \leq j \leq \lfloor \ell \rfloor - 1$ , and let

$$\varepsilon_{\lfloor \ell \rfloor} = \varepsilon_0 \left( \lceil \lfloor \ell \rfloor \frac{n}{\ell} \rceil, n \right),$$

where  $\varepsilon_0(x, y)$  is the error term defined in Lemma 5.2. Then we have

$$A_{n,0} = \ln \left( \frac{\ell^{\lfloor \ell \rfloor}}{\lfloor \ell \rfloor!} \right) - \sum_{j=1}^{\lfloor \ell \rfloor - 1} j \left[ \ln \left( \frac{\lceil (j+1) \frac{n}{\ell} \rceil - 1}{\lceil j \frac{n}{\ell} \rceil} \right) + \varepsilon_j \right] - \lfloor \ell \rfloor \left[ \ln \left( \frac{n}{\lceil \lfloor \ell \rfloor \frac{n}{\ell} \rceil} \right) + \varepsilon_{\lfloor \ell \rfloor} \right].$$

At this point, it will be convenient to split the error  $A_{n,0}$  into two pieces. Let  $D_1$  represent the difference between  $\lim_{n \rightarrow \infty} E[X_{n,0}]$  and the sum of the logarithms, and let  $D_2$  represent the sum of the terms involving the  $\varepsilon_j$ 's. That is, let

$$D_1 = \ln \left( \frac{\ell^{\lfloor \ell \rfloor}}{\lfloor \ell \rfloor!} \right) - \left[ \sum_{j=1}^{\lfloor \ell \rfloor - 1} j \ln \left( \frac{\lceil (j+1) \frac{n}{\ell} \rceil - 1}{\lceil j \frac{n}{\ell} \rceil} \right) + \lfloor \ell \rfloor \ln \left( \frac{n}{\lceil \lfloor \ell \rfloor \frac{n}{\ell} \rceil} \right) \right] \tag{60}$$

and

$$D_2 = \sum_{j=1}^{\lfloor \ell \rfloor} j \varepsilon_j. \quad (61)$$

Then we have  $A_{n,0} = D_1 - D_2$ . We will prove the following bounds for  $D_1$  and  $D_2$ :

**Lemma 7.1** *If  $n \geq \ell \geq 1$ , then*

$$0 < D_1 < \frac{3\ell^2}{n},$$

and

$$0 < D_2 \leq \frac{\ell^2}{n}.$$

Therefore, since  $A_{n,0} = D_1 - D_2$ ,

$$|A_{n,0}| \leq \frac{3\ell^2}{n}.$$

**Proof.** First note that the conditions imposed on  $\ell$  and  $n$  are merely the same conditions that ensure that the random variable  $X_{n,0}$  has nontrivial behavior. (Recall that if  $\ell < 1$ , then  $X_{n,0} = 0$  and so  $A_{n,0} = 0$ .) The first step in deriving the bounds on  $D_1$  and  $D_2$  is to bound the sequences that appear as limits on the sums in  $k$  from (59). Using the definition for ceiling, these bounds are

$$\frac{jn}{\ell} \leq \left\lceil \frac{jn}{\ell} \right\rceil < \frac{jn}{\ell} + 1, \quad (62)$$

$$\frac{(j+1)n}{\ell} - 1 \leq \left\lfloor \frac{(j+1)n}{\ell} \right\rfloor - 1 < \frac{(j+1)n}{\ell}, \quad (63)$$

$$\frac{\lfloor \ell \rfloor n}{\ell} \leq \left\lceil \frac{\lfloor \ell \rfloor n}{\ell} \right\rceil < \frac{\lfloor \ell \rfloor n}{\ell} + 1. \quad (64)$$

Now we consider the term  $D_1$ . Because of the conditions on  $\ell$ ,  $n$ , and  $j$ , each of the above quantities is positive. Therefore, these inequalities can be used to bound the individual logarithms in (60):

$$\ln \left( \frac{(j+1)\frac{n}{\ell} - 1}{j\frac{n}{\ell} + 1} \right) < \ln \left( \frac{\left\lceil \frac{(j+1)n}{\ell} \right\rceil - 1}{\left\lceil \frac{jn}{\ell} \right\rceil} \right) < \ln \left( \frac{j+1}{j} \right), \quad (65)$$

and

$$\ln \left( \frac{n}{\lfloor \ell \rfloor \frac{n}{\ell} + 1} \right) < \ln \left( \frac{n}{\left\lceil \frac{\lfloor \ell \rfloor n}{\ell} \right\rceil} \right) \leq \ln \left( \frac{\ell}{\lfloor \ell \rfloor} \right). \quad (66)$$

Now, recall from (32) that

$$\sum_{j=1}^{\lfloor \ell \rfloor - 1} j \ln \left( \frac{j+1}{j} \right) + \lfloor \ell \rfloor \ln \left( \frac{\ell}{\lfloor \ell \rfloor} \right) = \ln \left( \frac{\ell^{\lfloor \ell \rfloor}}{\lfloor \ell \rfloor!} \right). \quad (67)$$

Thus, the upper bounds on the individual terms are exactly what is needed to produce  $\lim_{n \rightarrow \infty} E[X_{n,0}]$  when added together. This will result in a lower bound of zero for  $D_1$ . The following discussion gives the specifics of translating inequalities (65) and (66) into an inequality on  $D_1$ .

In order to bound the entire quantity  $D_1$  using (65) and (66), we first factor the arguments of the logarithms that appear as lower bounds. In the case of the logarithm in (65), we have

$$\frac{(j+1)\frac{n}{\ell} - 1}{\frac{jn}{\ell} + 1} = \frac{(j+1) \left( 1 - \frac{\ell}{n(j+1)} \right)}{j \left( 1 + \frac{\ell}{nj} \right)}. \quad (68)$$

Thus, inequality (65) becomes

$$\ln \left( \frac{j+1}{j} \right) + \ln \left( \frac{1 - \frac{\ell}{n(j+1)}}{1 + \frac{\ell}{nj}} \right) < \ln \left( \frac{\lceil (j+1)\frac{n}{\ell} \rceil - 1}{\lceil j\frac{n}{\ell} \rceil} \right) < \ln \left( \frac{j+1}{j} \right), \quad (69)$$

which leads to

$$0 < \ln \left( \frac{j+1}{j} \right) - \ln \left( \frac{\lceil (j+1)\frac{n}{\ell} \rceil - 1}{\lceil j\frac{n}{\ell} \rceil} \right) < \ln \left( 1 + \frac{\ell}{nj} \right) - \ln \left( 1 - \frac{\ell}{n(j+1)} \right). \quad (70)$$

A similar argument shows that (66) can be rewritten as

$$0 \leq \ln \left( \frac{\ell}{\lfloor \ell \rfloor} \right) - \ln \left( \frac{n}{\lceil \lfloor \ell \rfloor \frac{n}{\ell} \rceil} \right) < \ln \left( 1 + \frac{\ell}{n\lfloor \ell \rfloor} \right). \quad (71)$$

Now, using (60) and (67), inequalities (70) and (71) lead directly to

$$0 < D_1 < \sum_{j=1}^{\lfloor \ell \rfloor - 1} j \left[ \ln \left( 1 + \frac{\ell}{nj} \right) - \ln \left( 1 - \frac{\ell}{n(j+1)} \right) \right] + \lfloor \ell \rfloor \ln \left( 1 + \frac{\ell}{n\lfloor \ell \rfloor} \right). \quad (72)$$

The bound in (72) can be simplified by observing that each term in the sum has the form  $\ln(1+x)$  or  $\ln(1-x)$ , where  $x$  is an expression involving  $\ell$ ,  $n$ , and  $j$ . Using the inequalities

$\ln(1+x) < x$  (valid for all  $x > 0$ ) and  $|\ln(1-x)| < 2x$  (valid for  $0 < x < 0.796\dots$ ), and noting that  $x \leq 1/2 < 0.796\dots$  for all terms involving  $\ln(1-x)$ , we have

$$0 < D_1 < \sum_{j=1}^{\lfloor \ell \rfloor - 1} \left[ \frac{\ell}{n} + \frac{2\ell}{n} \left( \frac{j}{j+1} \right) \right] + \frac{\ell}{n}, \quad (73)$$

or

$$0 < D_1 < \frac{\ell \lfloor \ell \rfloor}{n} + \frac{2\ell}{n} \sum_{j=1}^{\lfloor \ell \rfloor - 1} \left( \frac{j}{j+1} \right). \quad (74)$$

This obviously implies that

$$0 < D_1 < \frac{3\ell \lfloor \ell \rfloor}{n} \leq \frac{3\ell^2}{n}, \quad (75)$$

which proves the first inequality in Lemma 7.1.

Now we consider the term  $D_2$ ; recall that

$$D_2 = \sum_{j=1}^{\lfloor \ell \rfloor} j \varepsilon_j. \quad (76)$$

First we apply Lemma 5.2 to obtain bounds on the  $\varepsilon_j$ 's. For simplicity, we will use  $\varepsilon_j > 0$  as the lower bound; combining Lemma 5.2 with the inequalities in (62) and (64),

$$0 < \varepsilon_j \leq \frac{\ell}{nj}. \quad (77)$$

Applying these bounds to (76) we have

$$0 < D_2 \leq \sum_{j=1}^{\lfloor \ell \rfloor} \frac{\ell}{n} = \frac{\ell \lfloor \ell \rfloor}{n} \leq \frac{\ell^2}{n}, \quad (78)$$

which is the second inequality in Lemma 7.1.  $\square$

## 7.2 The Error for Rational $a$ in General

For a general rational number  $a$ , the total error  $A_{n,a}$  from (58) has an extra term,

$$A'_{n,a} = \lim_{n \rightarrow \infty} V_n(a, \ell) - V_n(a, \ell). \quad (79)$$

This section will be spent finding bounds for  $A'_{n,a}$ . Although some of the details are more complicated, the argument used below parallels the one used to bound  $A_{n,0}$ .

Using the definition (41) of  $V_n(a, \ell)$ , and recalling that  $\lfloor q\ell \rfloor - q\lfloor \ell \rfloor = \lfloor q\{\ell\} \rfloor$ ,

$$A'_{n,a} = \lim_{n \rightarrow \infty} V_n(a, \ell) - \left[ \sum_{i=1}^{q-1} \sum_{j=0}^{\lfloor \ell \rfloor - 1} \frac{1}{q} \sum_{k'=L_{n,ij}}^{M_{n,ij}} \frac{1}{k' + \frac{w_i}{q}} + \sum_{i=1}^{\lfloor q\{\ell\} \rfloor} \frac{1}{q} \sum_{k'=L'_{n,i}}^{M'_{n,i}} \frac{1}{k' + \frac{w_i}{q}} \right]. \quad (80)$$

For convenience, set  $u_i = w_i/q$ . Applying Lemma 5.2, we have

$$A'_{n,a} = \lim_{n \rightarrow \infty} V_n(a, \ell) \quad (81)$$

$$- \sum_{i=1}^{q-1} \sum_{j=0}^{\lfloor \ell \rfloor - 1} \frac{1}{q} \left[ \ln \left( \frac{M_{n,ij} + u_i}{L_{n,ij} + u_i} \right) + \epsilon_{u_i}(L_{n,ij}, M_{n,ij}) \right] \quad (82)$$

$$- \sum_{i=1}^{\lfloor q\{\ell\} \rfloor} \frac{1}{q} \left[ \ln \left( \frac{M'_{n,i} + u_i}{L'_{n,i} + u_i} \right) + \epsilon_{u_i}(L'_{n,i}, M'_{n,i}) \right]. \quad (83)$$

$$= E_1 - E_2, \quad (84)$$

where

$$E_1 = \lim_{n \rightarrow \infty} V_n(a, \ell) - \left[ \sum_{i=1}^{q-1} \sum_{j=0}^{\lfloor \ell \rfloor - 1} \frac{1}{q} \ln \left( \frac{M_{n,ij} + u_i}{L_{n,ij} + u_i} \right) + \sum_{i=1}^{\lfloor q\{\ell\} \rfloor} \frac{1}{q} \ln \left( \frac{M'_{n,i} + u_i}{L'_{n,i} + u_i} \right) \right] \quad (85)$$

and

$$E_2 = \sum_{i=1}^{q-1} \sum_{j=0}^{\lfloor \ell \rfloor - 1} \frac{1}{q} \epsilon_{u_i}(L_{n,ij}, M_{n,ij}) + \sum_{i=1}^{\lfloor q\{\ell\} \rfloor} \frac{1}{q} \epsilon_{u_i}(L'_{n,i}, M'_{n,i}). \quad (86)$$

We will prove the following, recalling the definition of  $H_m$  from Section 5:

**Lemma 7.2** *If  $\ell \geq 1/q$  and  $n \geq \max\{2q, 2\ell(q+1)\}$ , then*

$$0 < E_1 < \frac{2q(\ell^2 + \ell)}{n} (\ln q + 1) + \frac{2\ell q}{n} H_{\lfloor \ell \rfloor} + \frac{2q}{n}$$

and

$$0 < E_2 \leq \frac{q(\ell^2 + \ell)}{n} (\ln q + 1).$$

Therefore, since  $A'_{n,a} = E_1 - E_2$ ,

$$|A'_{n,a}| \leq \frac{2q(\ell^2 + \ell)}{n} (\ln q + 1) + \frac{2\ell q}{n} H_{\lfloor \ell \rfloor} + \frac{2q}{n}.$$

**Remark.** The requirement  $\ell \geq 1/q$  merely guarantees that  $X_{n,a}$  is nontrivial; if  $\ell < 1/q$ , then  $X_{n,a}$ ,  $A_{n,a}$ , and  $A'_{n,a}$  are all equal to 0. However, notice that in contrast to Lemma 7.1, there are nontrivial restrictions placed on  $n$  in Lemma 7.2.

**Proof.** The first step will be to derive bounds on the quantities  $L_{n,ij} + u_i$ ,  $M_{n,ij} + u_i$ , and so on. Recalling that  $u_i = w_i/q$ , equations (42) through (45) lead to the following inequalities:

$$\left(j + \frac{i}{q}\right) \frac{n}{q\ell} \leq L_{n,ij} + u_i < \left(j + \frac{i}{q}\right) \frac{n}{q\ell} + \frac{1}{q} + 1, \quad (87)$$

$$(j+1) \frac{n}{q\ell} - \frac{1}{q} - 1 < M_{n,ij} + u_i < (j+1) \frac{n}{q\ell}, \quad (88)$$

$$\left(\lfloor \ell \rfloor + \frac{i}{q}\right) \frac{n}{q\ell} \leq L'_{n,i} + u_i < \left(\lfloor \ell \rfloor + \frac{i}{q}\right) \frac{n}{q\ell} + \frac{1}{q} + 1, \quad (89)$$

$$\frac{n}{q} - 1 < M'_{n,i} + u_i \leq \frac{n}{q}. \quad (90)$$

An inspection of (88) and (90) reveals that these inequalities provide lower bounds on  $M_{n,ij} + u_i$  and  $M'_{n,i} + u_i$  that may be negative if  $n$  is too small. Assuming that  $n > q$  and  $n > (q+1)\ell$  ensures that all the relevant quantities are positive. (These conditions are guaranteed by the assumptions of Lemma 7.2.)

Now we consider the term  $E_1$ ; we will first bound the individual logarithms in (85) using inequalities (87) through (90). (Note that in order to do this, we need all the bounds to be positive as mentioned above.) Applying the above inequalities to the logarithms yields

$$\ln \left( \frac{(j+1) \frac{n}{q\ell} - \frac{1}{q} - 1}{\left(j + \frac{i}{q}\right) \frac{n}{q\ell} + \frac{1}{q} + 1} \right) < \ln \left( \frac{M_{n,ij} + u_i}{L_{n,ij} + u_i} \right) < \ln \left( \frac{j+1}{j + \frac{i}{q}} \right), \quad (91)$$

and

$$\ln \left( \frac{\frac{n}{q} - 1}{\left(\lfloor \ell \rfloor + \frac{i}{q}\right) \frac{n}{q\ell} + \frac{1}{q} + 1} \right) < \ln \left( \frac{M'_{n,i} + u_i}{L'_{n,i} + u_i} \right) \leq \ln \left( \frac{\ell}{\lfloor \ell \rfloor + \frac{i}{q}} \right). \quad (92)$$

Recall from (50) that

$$\sum_{i=1}^{q-1} \sum_{j=0}^{\lfloor \ell \rfloor - 1} \frac{1}{q} \ln \left( \frac{j+1}{j + \frac{i}{q}} \right) + \sum_{i=1}^{\lfloor q\{\ell\} \rfloor} \frac{1}{q} \ln \left( \frac{\ell}{\lfloor \ell \rfloor + \frac{i}{q}} \right) = \lim_{n \rightarrow \infty} V_n(a, \ell), \quad (93)$$

which shows that  $E_1 > 0$ . Following the procedure used for  $D_1$  above, to find an upper bound on  $E_1$  we now factor the arguments of the logarithms that appear as lower bounds

in (91) and (92). In the case of (91), we have

$$\frac{(j+1)\frac{n}{q\ell} - \frac{1}{q} - 1}{\left(j + \frac{i}{q}\right)\frac{n}{q\ell} + \frac{1}{q} + 1} = \frac{(j+1)\left[1 - \frac{\ell}{n}\left(\frac{1+q}{j+1}\right)\right]}{\left(j + \frac{i}{q}\right)\left[1 + \frac{\ell}{n}\left(\frac{1+q}{j + \frac{i}{q}}\right)\right]}, \quad (94)$$

which leads to

$$0 < \ln\left(\frac{j+1}{j + \frac{i}{q}}\right) - \ln\left(\frac{M_{n,ij} + u_i}{L_{n,ij} + u_i}\right) < \ln\left[1 + \frac{\ell}{n}\left(\frac{1+q}{j + \frac{i}{q}}\right)\right] - \ln\left[1 - \frac{\ell}{n}\left(\frac{1+q}{j+1}\right)\right]. \quad (95)$$

After a similar rearrangement of the terms, (92) becomes

$$0 \leq \ln\left(\frac{\ell}{[\ell] + \frac{i}{q}}\right) - \ln\left(\frac{M'_{n,i} + u_i}{L'_{n,i} + u_i}\right) < \ln\left[1 + \frac{\ell}{n}\left(\frac{1+q}{[\ell] + \frac{i}{q}}\right)\right] - \ln\left(1 - \frac{q}{n}\right). \quad (96)$$

Thus, applying (85) and (93), inequalities (95) and (96) result in

$$\begin{aligned} 0 < E_1 < & \sum_{i=1}^{q-1} \sum_{j=0}^{[\ell]-1} \frac{1}{q} \left( \ln\left[1 + \frac{\ell}{n}\left(\frac{1+q}{j + \frac{i}{q}}\right)\right] - \ln\left[1 - \frac{\ell}{n}\left(\frac{1+q}{j+1}\right)\right] \right) \\ & + \sum_{i=1}^{[q\{\ell\}]} \frac{1}{q} \left( \ln\left[1 + \frac{\ell}{n}\left(\frac{1+q}{[\ell] + \frac{i}{q}}\right)\right] - \ln\left(1 - \frac{q}{n}\right) \right). \end{aligned}$$

We can again use the inequalities  $\ln(1+x) < x$  and  $|\ln(1-x)| < 2x$  (for  $x < 0.796\dots$ ) to simplify the upper bound. The requirements  $n \geq 2q$  and  $n \geq 2\ell(q+1)$  of Lemma 7.2 ensure that  $x \leq 1/2 < 0.796\dots$  in all relevant cases. Using these approximations, we have

$$0 < E_1 < \sum_{i=1}^{q-1} \sum_{j=0}^{[\ell]-1} \frac{1}{q} \left[ \frac{\ell}{n} \left( \frac{1+q}{j + \frac{i}{q}} \right) + \frac{2\ell}{n} \left( \frac{1+q}{j+1} \right) \right] + \sum_{i=1}^{[q\{\ell\}]} \frac{1}{q} \left[ \frac{\ell}{n} \left( \frac{1+q}{[\ell] + \frac{i}{q}} \right) + \frac{2q}{n} \right]. \quad (97)$$

Consider the first sum in (97). We have

$$\sum_{i=1}^{q-1} \sum_{j=0}^{[\ell]-1} \frac{\ell}{qn} \left( \frac{1+q}{j + \frac{i}{q}} \right) \leq \frac{(q+1)\ell[\ell]}{qn} \sum_{i=1}^{q-1} \frac{q}{i} \quad (98)$$

$$= \frac{q+1}{n} \ell[\ell] H_{q-1} \quad (99)$$

$$\leq \frac{2q\ell^2}{n} (\ln q + 1), \quad (100)$$

and

$$\sum_{i=1}^{q-1} \sum_{j=0}^{[\ell]-1} \frac{2\ell}{qn} \left( \frac{1+q}{j+1} \right) = \left( q - \frac{1}{q} \right) \frac{2\ell}{n} \sum_{j'=1}^{[\ell]} \frac{1}{j'} = \left( q - \frac{1}{q} \right) \frac{2\ell}{n} H_{[\ell]} < \frac{2q\ell}{n} H_{[\ell]}. \quad (101)$$

For the second sum,

$$\sum_{i=1}^{[q\{\ell\}]} \left[ \frac{\ell}{qn} \left( \frac{1+q}{[\ell] + \frac{i}{q}} \right) + \frac{2}{n} \right] \leq \sum_{i=1}^{q-1} \left[ \frac{\ell(q+1)}{ni} + \frac{2}{n} \right] \quad (102)$$

$$= \frac{(q+1)\ell}{n} H_{q-1} + \frac{2(q-1)}{n} \quad (103)$$

$$\leq \frac{2q\ell}{n} (\ln q + 1) + \frac{2q}{n}. \quad (104)$$

Combining all the terms gives

$$0 < E_1 \leq \frac{2q(\ell^2 + \ell)}{n} (\ln q + 1) + \frac{2\ell q}{n} H_{[\ell]} + \frac{2q}{n}, \quad (105)$$

which is the first inequality in Lemma 7.2.

Finally we consider the term  $E_2$ ; recall that

$$E_2 = \sum_{i=1}^{q-1} \sum_{j=0}^{[\ell]-1} \frac{1}{q} \epsilon_{u_i}(L_{n,ij}, M_{n,ij}) + \sum_{i=1}^{[q\{\ell\}]} \frac{1}{q} \epsilon_{u_i}(L'_{n,i}, M'_{n,i}). \quad (106)$$

We can use Lemma 5.2 and inequalities (87) through (90) to obtain upper bounds for the  $\epsilon$  terms (again replacing the lower bound in Lemma 5.2 with 0), resulting in

$$0 < \epsilon_{u_i}(L_{n,ij}, M_{n,ij}) \leq \frac{1}{\left( j + \frac{i}{q} \right) \frac{n}{q\ell}} \quad (107)$$

and

$$0 < \epsilon_{u_i}(L'_{n,i}, M'_{n,i}) \leq \frac{1}{\left( [\ell] + \frac{i}{q} \right) \frac{n}{q\ell}}. \quad (108)$$

Therefore,

$$0 < E_2 \leq \frac{\ell}{n} \sum_{i=1}^{q-1} \sum_{j=0}^{[\ell]-1} \frac{1}{j + \frac{i}{q}} + \frac{\ell}{n} \sum_{i=1}^{[q\{\ell\}]} \frac{1}{[\ell] + \frac{i}{q}}. \quad (109)$$

Arguments similar to those used for  $E_1$  imply that

$$\frac{\ell}{n} \sum_{i=1}^{q-1} \sum_{j=0}^{[\ell]-1} \frac{1}{j + \frac{i}{q}} \leq \frac{q\ell^2}{n} (\ln q + 1) \quad (110)$$

and

$$\frac{\ell}{n} \sum_{i=1}^{\lfloor q^{\{\ell\}} \rfloor} \frac{1}{\lfloor \ell \rfloor + \frac{i}{q}} \leq \frac{q\ell}{n} (\ln q + 1). \quad (111)$$

Thus

$$0 < E_2 \leq \frac{q(\ell^2 + \ell)}{n} (\ln q + 1). \quad \square \quad (112)$$

### 7.3 The Total Error Bound

Together, Lemmas 7.1 and 7.2 immediately imply the following bound on the total error.

**Corollary 7.3** *Let  $a = p/q$  in lowest terms. If  $n \geq \max\{2q, 2\ell(q+1)\}$ , then*

$$|A_{n,a}| < \frac{2q \ln q}{n} (\ell^2 + \ell) + \frac{2q}{n} (\ell^2 + \ell + \ell H_{\lfloor \ell \rfloor} + 1) + \frac{3\ell^2}{n}.$$

This error bound can be simplified into a form that is slightly easier to work with. The following version of the bound will be used in Section 8.3.

**Theorem 7.4** *Let  $a = p/q$  in lowest terms. If  $n \geq \max\{2q, 2\ell(q+1)\}$ , then*

$$|A_{n,a}| < 16(1 + \ell^2) \frac{1 + q \ln q}{n}.$$

**Proof.** Suppose that  $n \geq \max\{2q, 2\ell(q+1)\}$ . Corollary 7.3 implies that if  $\ell < 1$ , then

$$|A_{n,a}| < 6 \frac{q \ln q + q + 1}{n},$$

and if  $\ell \geq 1$ , then

$$|A_{n,a}| < 8\ell^2 \frac{q \ln q + q + 1}{n}.$$

(Note that  $H_0 = 0$  and that  $\ell H_{\lfloor \ell \rfloor} \leq \ell(1 + \ln \ell) \leq \ell^2$ .) In either case we have

$$|A_{n,a}| < 8(1 + \ell^2) \frac{q \ln q + q + 1}{n}.$$

Finally, observe that  $q \leq 1 + q \ln q$ , so  $q \ln q + q + 1 \leq 2(1 + q \ln q)$ , proving the theorem.

□

## 8 The Mean When $a$ is Irrational

The second part of Theorem 1.1 will be proved in this section. We begin by stating that theorem more precisely. Let  $\mathcal{S}$  be the set of all numbers in  $[0, 1)$  defined as follows. A number  $a$  is in  $\mathcal{S}$  if and only if there exists a positive constant  $c$  (depending on  $a$ ) such that the inequality

$$\left| a - \frac{p}{q} \right| < \frac{c}{q^2 \ln^2(1+q)} \quad (113)$$

has no solutions in integers  $p$  and  $q$ . The theorem we will prove is the following:

**Theorem 8.1** *Suppose that  $a \in \mathcal{S}$ . Then*

$$\lim_{n \rightarrow \infty} E[X_{n,a}] = \ell.$$

The fact that  $\mathcal{S}$  includes all but a set of measure zero is the content of Corollary 8.9 below.

Based on Figure 1, it was observed at the end of Section 6 that for rational  $a = p/q$ , the larger the denominator  $q$  is, the closer the limiting function appears to be to the line  $f(\ell) = \ell$ . This observation gives the basic idea of the proof. We will take a sequence of rational numbers  $(r_n/s_n)$  approaching the irrational number  $a$ , and the random variable  $X_{n,a}$  will be approximated by  $X_{n, \frac{r_n}{s_n}}$ . Explicitly, for a given sequence  $(r_n/s_n)$  we have

$$\begin{aligned} |E[X_{n,a}] - \ell| &\leq \left| E[X_{n,a}] - E\left[X_{n, \frac{r_n}{s_n}}\right] \right| \\ &+ \left| E\left[X_{n, \frac{r_n}{s_n}}\right] - \frac{1}{s_n} \ln \left( \frac{(s_n \ell)^{\lfloor s_n \ell \rfloor}}{\lfloor s_n \ell \rfloor!} \right) \right| \\ &+ \left| \frac{1}{s_n} \ln \left( \frac{(s_n \ell)^{\lfloor s_n \ell \rfloor}}{\lfloor s_n \ell \rfloor!} \right) - \ell \right|. \end{aligned} \quad (114)$$

In order to prove Theorem 8.1, it will suffice to show that if  $a \in \mathcal{S}$ , then there exists a sequence  $(r_n/s_n)$  such that each of the three terms on the right-hand side of inequality (114) goes to zero as  $n \rightarrow \infty$ .

We will begin this section by defining the continued fraction expansion of an irrational number and discussing some basic properties of irrational numbers. We will use these ideas to explain how the sequence  $(r_n/s_n)$  is defined. We will then show that for  $a \in \mathcal{S}$ , each of the terms in (114) goes to zero. The first term requires careful use of the specific properties of the irrational number  $a$  (which is where the set  $\mathcal{S}$  comes in). The second term uses the rate of convergence results from Section 7. The third term is an easy consequence of Stirling's formula.

## 8.1 Continued Fractions and Approximation by Rational Numbers

This section covers some background information about continued fractions. The results presented here can be found in the book *Continued Fractions* by Khinchin [4], which provides a nice introduction to the subject.

As mentioned earlier, we will need to approximate an irrational number  $a$  with a sequence of rational numbers. In order to do so, we will make use of the notion of a best approximator.

**Definition 8.2 (Best Approximations)** Let  $\alpha$  be a real number, and let  $p/q$  be a fraction in lowest terms (with  $q > 0$ ).

1. If the inequality

$$\left| \alpha - \frac{r}{s} \right| > \left| \alpha - \frac{p}{q} \right|$$

holds for any integers  $r$  and  $s$  such that  $0 < s \leq q$  and  $r/s \neq p/q$ , then  $p/q$  is said to be a *best approximation of the first kind* for the number  $\alpha$ .

2. If the inequality

$$|s\alpha - r| > |q\alpha - p|$$

holds for any integers  $r$  and  $s$  such that  $0 < s \leq q$  and  $r/s \neq p/q$ , then  $p/q$  is said to be a *best approximation of the second kind* for the number  $\alpha$ .

Thus, a rational number  $p/q$  is best approximation of the first kind if it is closer to  $\alpha$  than any other rational number with a denominator that does not exceed  $q$ . It is a best approximation of the second kind only if the  $q^{\text{th}}$  multiple of  $\alpha$  comes closer to an integer than any previous multiple. It is easy to show that every best approximation of the second kind must be a best approximation of the first kind. However, the converse is not true. A best approximation of the first kind may fail to be a best approximation of the second kind.

The method of continued fractions turns out to provide a means to find the best approximations of a number. Since we are only interested in approximating irrational numbers, we will focus on the continued fraction representation of irrationals. We begin with some basic definitions.

**Definition 8.3 (Continued Fraction Expansion)** Given an irrational number  $\alpha$ , let

$$\begin{aligned} a_0 &= [\alpha] & , & & r_1 &= \frac{1}{\alpha - a_0} \\ a_1 &= [r_1] & , & & r_2 &= \frac{1}{r_1 - a_1} \\ &\vdots & & & \vdots & \\ a_k &= [r_k] & , & & r_{k+1} &= \frac{1}{r_k - a_k}. \end{aligned}$$

Since  $\alpha$  is irrational, this process never terminates, and it defines the  $a_k$  so that

$$\alpha = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \dots}}$$

and  $a_k \geq 1$  for  $k \geq 1$ . This representation is called the *continued fraction expansion* of  $\alpha$ , and we will denote it by

$$\alpha = [a_0; a_1, a_2, \dots].$$

The  $a_k$  are called the *elements* of the number  $\alpha$ . The number  $r_k$  is called the  $k^{\text{th}}$  *remainder* of  $\alpha$  and its continued fraction expansion is  $[a_k; a_{k+1}, a_{k+2}, \dots]$ .

**Definition 8.4 (Convergents)** Given  $\alpha = [a_0; a_1, a_2, \dots]$ , define sequences  $p_k$  and  $q_k$  by

$$\begin{aligned} p_{-1} &= 1 & , & & q_{-1} &= 0 \\ p_0 &= a_0 & , & & q_0 &= 1 \\ p_1 &= a_1 p_0 + 1 & , & & q_1 &= a_1 \\ &\vdots & & & \vdots & \\ p_k &= a_k p_{k-1} + p_{k-2} & , & & q_k &= a_k q_{k-1} + q_{k-2}. \end{aligned}$$

The integers  $p_k$  and  $q_k$  are relatively prime for each  $k$ , and the fractions  $p_k/q_k$  are called the *convergents* of  $\alpha$ .

**Remark.** Definitions 8.3 and 8.4 apply equally well to rational numbers, except that the continued fraction expansion of rationals is finite.

The next theorem shows why the convergents are important. It is essentially the content of Theorems 16 and 17 in [4] (pp. 24-28).

**Theorem 8.5** *Every best approximation of the second kind for a number  $\alpha$  is a convergent of  $\alpha$ . Furthermore, every convergent is a best approximation of the second kind, with the exception of the  $0^{\text{th}}$  order convergent of any  $\alpha$  whose fractional part is greater than or equal to  $1/2$ .*

**Remark.** If  $a_0 + 1/2 \leq \alpha < a_0 + 1$ , then  $p_0/q_0 = a_0/1$  is not a best approximation of the first kind (and hence not of the second kind either) since

$$\left| \alpha - \frac{a_0}{1} \right| \geq \frac{1}{2} \geq \left| \alpha - \frac{a_0 + 1}{1} \right|.$$

Definition 8.4 and Theorem 8.5 show that the convergents of order greater than 0 form a sequence of best approximations whose denominators are strictly increasing. We will be primarily interested in the convergents' property of being best approximations of the first kind rather than of the second kind. Although there may be other rational numbers that are first-kind approximators, the convergents have additional properties that will be useful to us. The following theorem presents another result that we will need.

**Theorem 8.6** *For any irrational  $\alpha$  and for all  $k \geq 0$ ,*

$$\frac{1}{q_k(q_k + q_{k+1})} < \left| \alpha - \frac{p_k}{q_k} \right| < \frac{1}{q_k q_{k+1}}.$$

For proofs of these bounds, see [4], Theorems 9 and 13 (pp. 9, 21).

Often, it is of interest to evaluate the closeness of an approximation by comparing the difference  $|\alpha - p/q|$  with some decreasing function of the denominator  $q$ . Notice that, since the  $q_k$  are increasing, Theorem 8.6 implies the inequality

$$\left| \alpha - \frac{p_k}{q_k} \right| < \frac{1}{q_k^2} \tag{115}$$

for all  $\alpha$  and all  $k \geq 0$ . Thus, every irrational number admits approximations on the order of  $1/q^2$  for infinitely many rational numbers  $p/q$ . The next theorem shows that if the continued fraction expansion of  $\alpha$  has bounded elements, this is essentially the highest order of approximation that can be achieved, whereas irrationals with unbounded elements admit closer approximations. This theorem is taken directly from [4], Theorem 23 (p. 36).

**Theorem 8.7** *For every irrational number  $\alpha$  with bounded elements, there is a positive constant  $c$  depending on  $\alpha$  such that the inequality*

$$\left| \alpha - \frac{p}{q} \right| < \frac{c}{q^2} \quad (116)$$

*has no solution in integers  $p$  and  $q$ . On the other hand, for every number  $\alpha$  with an unbounded sequence of elements and arbitrary  $c > 0$ , inequality (116) has an infinite set of such solutions.*

**Remark.** The constant  $c$  in Theorem 8.7 must be less than  $1/\sqrt{5}$ . If  $c \geq 1/\sqrt{5}$ , then for any irrational  $\alpha$ , inequality (116) has infinitely many solutions. (See [4], Theorem 21, p. 34.)

It is worthwhile to point out that, included in the set of irrationals with bounded elements are all quadratic irrationals, which are in fact characterized by having a periodic sequence of elements. We also note that Theorem 8.7 implies that irrationals with bounded elements are included in the set  $\mathcal{S}$  defined at the beginning of Section 8. To see this, suppose that there exists  $c_1$  so that (116) has no solution in integers  $p$  and  $q$ . Then choosing any constant  $c_2 \leq c_1 \ln^2 2$  for inequality (113) ensures that it will likewise have no solution.

As one might imagine, there are many more numbers whose sequence of elements is unbounded than there are numbers whose elements form a bounded sequence. In fact, it can be shown (see [4], Theorem 29, p. 60) that the set of numbers in the interval  $[0, 1)$  with bounded elements has measure 0. While Theorem 8.7 only holds for irrationals with bounded elements, there is a general result that holds for a much larger class of irrationals. This is Theorem 32 from [4] (p. 69).

**Theorem 8.8** *Suppose that  $f(x)$  is a positive continuous function of a positive variable  $x$  and that  $xf(x)$  is a non-increasing function. Then for almost all  $\alpha \in [0, 1)$  (i.e., except for a set of measure 0), the inequality*

$$\left| \alpha - \frac{p}{q} \right| < \frac{f(q)}{q} \quad (117)$$

*has only a finite number of solutions in integers  $p$  and  $q$  (with  $q > 0$ ) if, for some  $c > 0$ , the integral*

$$\int_c^\infty f(x) dx \quad (118)$$

converges. On the other hand, for almost all  $\alpha \in [0, 1)$ , inequality (117) has an infinite set of solutions in integers  $p$  and  $q$  (with  $q > 0$ ) if the integral (118) diverges.

The first half of Theorem 8.8 implies the following result.

**Corollary 8.9** *For almost all  $\alpha \in [0, 1)$ , there is a positive constant  $c$  depending on  $\alpha$  such that the inequality*

$$\left| \alpha - \frac{p}{q} \right| < \frac{c}{q^2 \ln^2(1+q)} \quad (119)$$

has no solution in integers  $p$  and  $q$ . Thus, the set  $\mathcal{S}$  has measure 1.

**Proof.** By the first part of Theorem 8.8, for almost all irrational numbers  $\alpha$ , the inequality

$$\left| \alpha - \frac{p}{q} \right| < \frac{1}{q^2 \ln^2(1+q)}$$

has only a finite number of solutions in integers  $p$  and  $q$ . Let  $\alpha$  be such an irrational number, and choose any  $c$  such that

$$0 < c < \min \left\{ \left| \alpha - \frac{p}{q} \right| : \left| \alpha - \frac{p}{q} \right| < \frac{1}{q^2 \ln^2(1+q)}, p, q \in \mathbb{Z} \right\}.$$

For such a  $c$ , inequality (119) clearly has no solution in integers  $p$  and  $q$ , which shows that  $\alpha$  is in  $\mathcal{S}$  and hence that  $\mathcal{S}$  has measure 1.  $\square$

## 8.2 Approximating $I_n = (e^{2\pi ia}, e^{2\pi i(a+\ell/n)})$ with a Nearby Interval

Suppose that  $a = [a_0; a_1, a_2, \dots]$  is an irrational number, and let  $(p_k/q_k)$  be the sequence of convergents for  $a$ . For any positive integer  $n$ , choose  $k(n)$  to be the integer satisfying

$$q_{k(n)+1} \ln^2(q_{k(n)+1}) > n \geq q_{k(n)} \ln^2(q_{k(n)}), \quad (120)$$

and let  $r_n = p_{k(n)}$  and  $s_n = q_{k(n)}$ . Obviously, both  $k(n)$  and  $q_{k(n)}$  increase without bound as  $n \rightarrow \infty$ . Our goal is to approximate the random variable  $X_{n,a}$  with  $X_{n, \frac{r_n}{s_n}}$ ; thus we want to compare the number of eigenvalues in the interval

$$I_n = \left( e^{2\pi ia}, e^{2\pi i(a+\frac{\ell}{n})} \right) \quad (121)$$

with the number of eigenvalues in

$$I_n^* = \left( e^{2\pi i \left( \frac{r_n}{s_n} \right)}, e^{2\pi i \left( \frac{r_n}{s_n} + \frac{\ell}{n} \right)} \right). \quad (122)$$

When we shift the interval  $I_n$  to the nearby interval  $I_n^*$ , any eigenvalues that occur at rational points between the left or right endpoints of the intervals will be included in one interval but not the other. Hence, the difference between  $X_{n,a}$  and  $X_{n,\frac{r_n}{s_n}}$  will be the difference between the number of eigenvalues in these “gaps” between the two intervals. To make this precise, define intervals

$$J_{1,n} = \left( e^{2\pi i a}, e^{2\pi i \left(\frac{r_n}{s_n}\right)} \right] \quad (123)$$

and

$$J_{2,n} = \left( e^{2\pi i \left(a + \frac{\ell}{n}\right)}, e^{2\pi i \left(\frac{r_n}{s_n} + \frac{\ell}{n}\right)} \right] \quad (124)$$

if  $r_n/s_n > a$ , or

$$J_{1,n} = \left( e^{2\pi i \left(\frac{r_n}{s_n}\right)}, e^{2\pi i a} \right] \quad (125)$$

and

$$J_{2,n} = \left( e^{2\pi i \left(\frac{r_n}{s_n} + \frac{\ell}{n}\right)}, e^{2\pi i \left(a + \frac{\ell}{n}\right)} \right] \quad (126)$$

if  $r_n/s_n < a$ . Let  $Y_{1,n}$  and  $Y_{2,n}$  be random variables which count the number of eigenvalues in  $J_{1,n}$  and  $J_{2,n}$ , respectively. Then we have  $X_{n,a} - X_{n,\frac{r_n}{s_n}} = \pm (Y_{1,n} - Y_{2,n})$  (where, for a fixed  $n$ , the sign is the same for all  $\sigma \in S_n$ ), and so

$$\left| E[X_{n,a}] - E\left[X_{n,\frac{r_n}{s_n}}\right] \right| = |E[Y_{1,n}] - E[Y_{2,n}]| \leq \max(E[Y_{1,n}], E[Y_{2,n}]). \quad (127)$$

We will show that if  $a$  is in the set  $\mathcal{S}$  defined at the beginning of Section 8, then  $E[Y_{1,n}]$  and  $E[Y_{2,n}]$  both approach 0 as  $n \rightarrow \infty$ , and hence the mean of  $X_{n,a}$  approaches that of  $X_{n,\frac{r_n}{s_n}}$ . We proceed by proving several fairly straightforward facts which will allow us to bound  $E[Y_{1,n}]$  and  $E[Y_{2,n}]$ . The first of these is a bound on the growth rate of the denominators of the convergents for an irrational number in  $\mathcal{S}$ .

**Lemma 8.10** *Suppose that  $a \in \mathcal{S}$ . Then there exists a positive constant  $M$  depending on  $a$  such that for all  $k \geq 0$ ,*

$$q_{k+1} < Mq_k \ln^2(1 + q_k).$$

**Proof.** From the definition of  $\mathcal{S}$ , there exists  $c > 0$  such that

$$\left| a - \frac{p_k}{q_k} \right| \geq \frac{c}{q_k^2 \ln^2(1 + q_k)}$$

for all  $k \geq 0$ , and from Theorem 8.6, we have

$$\left| a - \frac{p_k}{q_k} \right| < \frac{1}{q_k q_{k+1}}$$

for all  $k \geq 0$ . Therefore,

$$\frac{c}{q_k^2 \ln^2(1 + q_k)} < \frac{1}{q_k q_{k+1}},$$

or

$$q_{k+1} < \frac{q_k \ln^2(1 + q_k)}{c} = M q_k \ln^2(1 + q_k),$$

where  $M = 1/c$ .  $\square$

Now we show that for  $a \in \mathcal{S}$ , the distance from  $a$  to the approximating rational  $r_n/s_n$  is eventually shorter than the length of the interval  $I_n$ .

**Lemma 8.11** *Let  $a \in \mathcal{S}$ . There exists a positive integer  $N_1$  depending on  $a$  such that for all  $n \geq N_1$ ,*

$$\left| a - \frac{r_n}{s_n} \right| < \frac{\ell}{n}.$$

**Proof.** It will suffice to show that

$$\lim_{n \rightarrow \infty} \left| a - \frac{r_n}{s_n} \right| \cdot \frac{n}{\ell} = 0.$$

Using Theorem 8.6 and Lemma 8.10,

$$\left| a - \frac{p_{k(n)}}{q_{k(n)}} \right| \cdot \frac{n}{\ell} < \frac{1}{q_{k(n)} q_{k(n)+1}} \cdot \frac{q_{k(n)+1} \ln^2(q_{k(n)+1})}{\ell} \leq \frac{\ln^2 [M q_{k(n)} \ln^2(1 + q_{k(n)})]}{\ell q_{k(n)}}. \quad (128)$$

The numerator in (128) increases as a polynomial in  $\ln(q_{k(n)})$ , while the denominator increases linearly with  $q_{k(n)}$ . Clearly, this expression approaches 0 as  $n$  (and hence  $q_{k(n)}$ ) approaches  $\infty$ .  $\square$

Next we obtain lower bounds on the denominators of the rational numbers that lie in the intervals  $J_{1,n}$  and  $J_{2,n}$ .

**Lemma 8.12** Let  $a \in \mathcal{S}$ . Define  $N_2 = \max\{N_1, q_2 \ln^2(q_2)\}$ , where  $N_1$  is the constant from Lemma 8.11, and suppose that  $n \geq N_2$ .

1. If  $u/v$  is a rational number satisfying

$$\left| a - \frac{u}{v} \right| \leq \left| a - \frac{r_n}{s_n} \right|,$$

then  $v \geq s_n$ .

2. Let  $M$  be the constant from Lemma 8.10. If  $u/v$  is a rational number satisfying

$$\left| a + \frac{\ell}{n} - \frac{u}{v} \right| \leq \left| a - \frac{r_n}{s_n} \right|,$$

then

$$v \geq \left( \frac{s_n}{2\ell M} \right)^{1/3} \ln^{2/3} s_n.$$

**Remark.** Note that the hypotheses in part 1 and part 2 were chosen so that the resulting bounds on  $v$  apply to all rational numbers in  $J_{1,n}$  and  $J_{2,n}$ , respectively.

**Proof.**

(Part 1). This follows directly from the fact that convergents of order greater than 0 are best approximations of the first kind.

(Part 2). Since  $n \geq N_1$ , it follows that

$$\left| a - \frac{u}{v} \right| \leq \left| a + \frac{\ell}{n} - \frac{u}{v} \right| + \frac{\ell}{n} \leq \left| a - \frac{r_n}{s_n} \right| + \frac{\ell}{n} < \frac{2\ell}{n},$$

and since  $a \in \mathcal{S}$ , there is a constant  $c > 0$  such that

$$\left| a - \frac{u}{v} \right| \geq \frac{c}{v^2 \ln^2(1+v)} > \frac{c}{v^3}.$$

Therefore,

$$\frac{c}{v^3} < \frac{2\ell}{n} \leq \frac{2\ell}{s_n \ln^2 s_n}. \quad (129)$$

The requirement  $n \geq q_2 \ln^2(q_2)$  ensures that  $s_n \geq q_2 > 1$  so that  $\ln(s_n) > 0$ . Inequality (129) leads directly to

$$v \geq \left( \frac{cs_n}{2\ell} \right)^{1/3} \ln^{2/3} s_n,$$

and using Lemma 8.10, we may substitute  $1/M$  for  $c$ .  $\square$

Finally we place a bound on the expected number of eigenvalues in any interval that only contains rational points with denominators larger than some known minimum value.

**Lemma 8.13** Let  $J = (e^{2\pi i x}, e^{2\pi i(x+y)})$  be any interval on the unit circle (with  $0 < y \leq 1$ ).

1. There are at most  $\lceil n^2 y \rceil$  rational numbers  $u/v$  with  $v \leq n$  such that  $e^{2\pi i u/v} \in J$ .
2. Let  $Y_n$  be the number of eigenvalues lying in  $J$  for a random  $n \times n$  permutation matrix, and define

$$m = \min\{v : e^{2\pi i u/v} \in J, u \in \mathbb{Z}, v \in \mathbb{N}\}.$$

Then

$$E[Y_n] \leq \lceil n^2 y \rceil \cdot \frac{1}{m} (\ln n + 1).$$

**Proof.**

(Part 1). For any two distinct rational numbers, both of which have denominators no bigger than  $n$ , the distance between them is at least  $1/n(n-1)$  (and is therefore greater than  $1/n^2$ ). The bound follows immediately.

(Part 2). Define  $J'$  to be the interval  $(x, x+y]$ . Then for an  $n \times n$  permutation matrix  $M_\sigma$ ,

$$Y_n(M_\sigma) = \sum_{\frac{u}{v} \in J'} \sum_{k:v|k} C_k(\sigma). \quad (130)$$

Thus

$$E[Y_n] = \sum_{\frac{u}{v} \in J'} \sum_{k:v|k} E[C_k(\sigma)] \quad (131)$$

$$= \sum_{\substack{\frac{u}{v} \in J' \\ v \leq n}} \sum_{k:v|k} \frac{1}{k} \quad (132)$$

$$= \sum_{\substack{\frac{u}{v} \in J' \\ v \leq n}} \sum_{k'=1}^{\lfloor n/v \rfloor} \frac{1}{vk'} \quad (133)$$

$$\leq \sum_{\substack{\frac{u}{v} \in J' \\ v \leq n}} \sum_{k'=1}^{\lfloor n/m \rfloor} \frac{1}{mk'} \quad (134)$$

$$\leq \lceil n^2 y \rceil \cdot \frac{1}{m} (\ln n + 1). \quad \square \quad (135)$$

The above lemmas lead directly to the following upper bounds for  $E[Y_{1,n}]$  and  $E[Y_{2,n}]$ .

**Lemma 8.14** *Let  $N_2$  be as defined in Lemma 8.12. If  $n \geq N_2$ , then*

$$E[Y_{1,n}] \leq \left\lceil \frac{n^2}{s_n^2} \right\rceil \frac{(\ln n + 1)}{s_n}$$

and

$$E[Y_{2,n}] \leq (2\ell M)^{1/3} \left\lceil \frac{n^2}{s_n^2} \right\rceil \frac{(\ln n + 1)}{s_n^{1/3} \ln^{2/3} s_n}.$$

**Proof.** First consider  $Y_{1,n}$ . The length of  $J_{1,n}$  is  $|a - r_n/s_n|$ , and from (115) we have

$$\left| a - \frac{r_n}{s_n} \right| < \frac{1}{s_n^2}. \quad (136)$$

From the first part of Lemma 8.12, we know that if  $u/v \in J_{1,n}$  then  $v \geq s_n$ , so by Lemma 8.13,

$$E[Y_1] \leq \left\lceil \frac{n^2}{s_n^2} \right\rceil \frac{(\ln n + 1)}{s_n}. \quad (137)$$

The second equation has essentially the same proof, using the second part of Lemma 8.12 combined with Lemma 8.13.  $\square$

At last we are ready to prove the main result.

**Theorem 8.15** *Let  $a$  be an element of the set  $\mathcal{S}$ , and for any integer  $n$ , let  $r_n$  and  $s_n$  be as defined above. Then*

$$\left| E[X_{n,a}] - E\left[X_{n, \frac{r_n}{s_n}}\right] \right| \rightarrow 0$$

as  $n \rightarrow \infty$ .

**Proof.** Based on (127) and the bounds in Lemma 8.14, proving the theorem amounts to proving that

$$\lim_{n \rightarrow \infty} \left( \left\lceil \frac{n^2}{s_n^2} \right\rceil \cdot \frac{(\ln n + 1)}{s_n^{1/3} \ln^{2/3} s_n} \right) = 0. \quad (138)$$

From the way  $k(n)$  and  $s_n$  were defined, we have

$$n < q_{k(n)+1} \ln^2(q_{k(n)+1})$$

and

$$s_n = q_{k(n)}.$$

Thus,

$$\left[ \frac{n^2}{s_n^2} \right] \cdot \frac{(\ln n + 1)}{s_n^{1/3} \ln^{2/3}(s_n)} \leq \left[ \left( \frac{q_{k(n)+1} \ln^2(q_{k(n)+1})}{q_{k(n)}} \right)^2 \right] \cdot \frac{\ln [q_{k(n)+1} \ln^2(q_{k(n)+1})] + 1}{q_{k(n)}^{1/3} \ln^{2/3}(q_{k(n)})}. \quad (139)$$

Now, using Lemma 8.10,

$$\left[ \left( \frac{q_{k(n)+1} \ln^2(q_{k(n)+1})}{q_{k(n)}} \right)^2 \right] \leq [M^2 \ln^4(1 + q_{k(n)})] \cdot \ln^4 [M q_{k(n)} \ln^2(1 + q_{k(n)})] + 1 \quad (140)$$

and

$$\frac{\ln [q_{k(n)+1} \ln^2(q_{k(n)+1})] + 1}{q_{k(n)}^{1/3} \ln^{2/3}(q_{k(n)})} \leq \frac{\ln [[M q_{k(n)} \ln^2(1 + q_{k(n)})] \cdot \ln^2 [M q_{k(n)} \ln^2(1 + q_{k(n)})]] + 1}{q_{k(n)}^{1/3} \ln^{2/3}(q_{k(n)})}. \quad (141)$$

When the right-hand sides of (140) and (141) are multiplied, the resulting expression has a numerator that is bounded above by some polynomial in  $\ln(q_{k(n)})$  and a denominator that grows faster than  $q_{k(n)}^{1/3}$ . Therefore the whole expression goes to zero as  $n \rightarrow \infty$ .  $\square$

### 8.3 The Convergence of $E[X_{n,a}]$ for $a \in \mathcal{S}$

Finally we prove the other two limits needed to complete the proof of Theorem 8.1.

**Theorem 8.16** *For any irrational number  $a$ , let  $r_n$  and  $s_n$  be defined as in the previous section, and let  $A_{n, \frac{r_n}{s_n}}$  be defined as in Section 7. Then*

$$\lim_{n \rightarrow \infty} A_{n, \frac{r_n}{s_n}} = 0.$$

**Proof.** Choose an integer  $N$  large enough so that

$$\ln^2(q_{k(N)}) \geq \max\{2, 4\ell\}, \quad (142)$$

and let  $n \geq N$ . Then since  $n \geq q_{k(n)} \ln^2(q_{k(n)})$ , we have

$$n \geq 2q_{k(n)} \quad (143)$$

and

$$n \geq 4\ell q_{k(n)} \geq 2\ell (q_{k(n)} + 1). \quad (144)$$

Therefore, for  $n \geq N$ , we may apply Theorem 7.4 to the error term  $A_{n, \frac{r_n}{s_n}}$  (recall that  $r_n/s_n = p_{k(n)}/q_{k(n)}$ ):

$$\left| A_{n, \frac{r_n}{s_n}} \right| < 16(1 + \ell^2) \frac{1 + s_n \ln(s_n)}{n} \quad (145)$$

$$\leq 16(1 + \ell^2) \frac{1 + q_{k(n)} \ln(q_{k(n)})}{q_{k(n)} \ln^2(q_{k(n)})} \quad (146)$$

$$= 16(1 + \ell^2) \left[ \frac{1}{q_{k(n)} \ln^2(q_{k(n)})} + \frac{1}{\ln(q_{k(n)})} \right]. \quad (147)$$

The two terms in (147) approach 0 as  $q_{k(n)} \rightarrow \infty$ , so

$$\lim_{n \rightarrow \infty} \left| A_{n, \frac{r_n}{s_n}} \right| = 0. \quad \square$$

**Theorem 8.17** For any positive real number  $\ell$ ,

$$\lim_{x \rightarrow \infty} \left[ \frac{1}{x} \ln \left( \frac{(x\ell)^{\lfloor x\ell \rfloor}}{\lfloor x\ell \rfloor!} \right) \right] = \ell. \quad (148)$$

**Proof.** In order to prove the limit (148), we make use of the following version of Stirling's formula (see p. 52 of [2]):

$$\lim_{N \rightarrow \infty} \frac{N^N e^{-N} \sqrt{2\pi N}}{N!} = 1. \quad (149)$$

In particular, we have

$$\begin{aligned} \frac{1}{x} \ln \left( \frac{(x\ell)^{\lfloor x\ell \rfloor}}{\lfloor x\ell \rfloor!} \right) &= \frac{1}{x} \ln \left( \frac{(x\ell)^{\lfloor x\ell \rfloor}}{\lfloor x\ell \rfloor^{\lfloor x\ell \rfloor} e^{-\lfloor x\ell \rfloor} \sqrt{2\pi \lfloor x\ell \rfloor}} \right) \\ &\quad + \frac{1}{x} \ln \left( \frac{\lfloor x\ell \rfloor^{\lfloor x\ell \rfloor} e^{-\lfloor x\ell \rfloor} \sqrt{2\pi \lfloor x\ell \rfloor}}{\lfloor x\ell \rfloor!} \right), \end{aligned} \quad (150)$$

and (149) implies that the second term in (150) goes to 0 as  $x \rightarrow \infty$ . Therefore,

$$\begin{aligned} \lim_{x \rightarrow \infty} \frac{1}{x} \ln \left( \frac{(x\ell)^{\lfloor x\ell \rfloor}}{\lfloor x\ell \rfloor!} \right) &= \lim_{x \rightarrow \infty} \frac{1}{x} \ln \left( \frac{(x\ell)^{\lfloor x\ell \rfloor}}{\lfloor x\ell \rfloor^{\lfloor x\ell \rfloor} e^{-\lfloor x\ell \rfloor} \sqrt{2\pi \lfloor x\ell \rfloor}} \right) \\ &= \lim_{x \rightarrow \infty} \left[ \frac{\lfloor x\ell \rfloor}{x} \ln \left( \frac{x\ell}{\lfloor x\ell \rfloor} \right) + \frac{\lfloor x\ell \rfloor}{x} - \frac{1}{x} \ln(\sqrt{2\pi \lfloor x\ell \rfloor}) \right] \\ &= \ell \cdot 0 + \ell - 0 \\ &= \ell. \quad \square \end{aligned}$$

Since all three terms in equation (114) converge to 0 as  $n \rightarrow \infty$ , we have proved Theorem 8.1 (which implies part 2 of Theorem 1.1).

## 9 Conclusion

There are a few generalizations of Theorem 1.1 which are easy to explain. First, the results derived in this paper are for half-open intervals, rather than for more standard open or closed intervals. This was done mainly to simplify notation as much as possible. In fact, the limit for an open interval of the form  $(e^{2\pi ia}, e^{2\pi i(a+\ell/n)})$  is the same as the limit for the half-open interval studied here. When  $a$  is irrational, the limit will be the same for closed intervals as well. However, it is easy to see that for rational  $a$ , including the lower endpoint will have a huge effect—the mean no longer would stay bounded because the number of eigenvalues at the endpoint  $a$  grows as  $\frac{1}{q} \ln n$ .

The set  $S$  can also be modified somewhat. For any real number  $\omega > 1$ , define  $S_\omega$  to be the set of all numbers  $a$  for which there exists a constant  $c$  (depending on  $a$ ) such that

$$\left| a - \frac{p}{q} \right| \leq \frac{c}{q^2 \ln^\omega(1+q)} \quad (151)$$

has no solutions in integers  $p$  and  $q$ . If  $\omega > 2$ , then  $S \subseteq S_\omega$ ; the proof of Theorem 8.1 can be modified to include irrational numbers  $a \in S_\omega$  for any  $\omega$ .

However, it is worth noting that the phrase “almost every” in Theorem 1.1 is necessary. Any irrational number which is not of finite type will not lie in any of the sets  $S_\omega$ . In fact, it can be shown that if  $a$  is an irrational number that can be approximated extremely well, then  $E[X_{n,a}]$  has an unbounded subsequence, so the mean cannot possibly converge to  $\ell$  (or any other finite value). Thus there exist irrationals to which Theorem 1.1 does not apply.

There are other questions about  $X_{n,a}$  which are still unanswered. Using the results of section 2.2, a formula can be derived for  $Var[X_{n,a}]$  in a way similar to what was done for the mean, although the sum is more complicated. Some work with this sum has shown that the variance is bounded for  $a = 0$ , and we suspect that it will be bounded for other values of  $a$  as well. It would be interesting to try to derive a formula for the limit of the variance, and more generally, to better understand the distribution of  $X_{n,a}$ .

## Acknowledgements

The author would like to thank Kelly Wieand for all her support and guidance on this project and for her assistance in writing and editing the paper.

## References

- [1] Diaconis, P. and Shahshahani, M., On the Eigenvalues of Random Matrices, *Journal of Applied Probability* **31** (1994), pp. 49-61
- [2] Feller, W., *An Intorduction to Probability Theory and Its Applications, vol. 1*, John Wiley and Sons, New York, 1968
- [3] Goncharov, V., Du domaine d'analyse Combinatoire, *Bull. Acad. Sci. USSR Ser. Mat.*, **8** (1944), pp. 3-48; *AMS Translations, Series 2*, **19** (1962), pp. 1-46
- [4] Khinchin, A. Ya., *Continued Fractions, 3rd ed.*, The University of Chicago Press, Chicago, 1964
- [5] Shepp, L. A. and Lloyd, S. P., Ordered Cycle Lengths in a Random Permutation, *Trans. AMS* **121** (1966), pp. 340-357
- [6] Wieand, K., *Eigenvalue Distributions of Random Matrices in the Permutation Group and Compact Lie Groups*, Ph. D. Thesis, Harvard University 1998
- [7] Wieand, K., Eigenvalue Distributions of Random Permutation Matrices, *Annals of Probability* **28** (2000), pp. 1563-1587