Factorization in $F_q[x]$ and Brownian motion

Jennie C. Hansen

Actuarial Mathematics and Statistics Department

Heriot-Watt University

Edinburgh, Scotland

Abstract. We consider the set of polynomials of degree n over a finite field and put the uniform probability measure on this set. Any such polynomial factors uniquely into a product of its irreducible factors. To each polynomial we associate a step function on the interval [0,1] such that the size of each jump corresponds to the number of factors of a certain degree in the factorization of the random polynomial. We normalize these random functions and show that the resulting random process converges weakly to Brownian motion as $n \to \infty$. This result complements earlier work by the author on the order statistics of the degree sequence of the factors of a random polynomial.

This research was partially supported by NSF grant DMS- 90 099074.

1. Introduction

In this paper we study the factorization of random polynomials over the finite field F_q, q a prime power. Specifically, let Π_n denote the monic polynomials of degree n over F_q and let μ_n denote the uniform measure on Π_n. Any $f(x) \in \Pi_n$ factors uniquely and the degrees of its factors determine a partition of the integer n. To investigate the limiting distribution of such partitions with respect to the measure μ_n as $n \to \infty$, we introduce the counting functions $\alpha_k : \bigcup_{n=1}^{\infty} \Pi_n \to Z$ defined by setting $\alpha_k(f)$ equal to the number of factors in f of degree k. Now let $p(n) = |\Pi_n| = q^n$ and let $c(n)$ denote the number of irreducible monic polynomials of degree n, then the joint distribution of $\alpha_1, \alpha_2, ...\alpha_n$ with respect to μ_n can be expressed in terms of $p(n)$ and $c(1), c(2), ..., c(n)$ as follows.

$$\mu_n(\alpha_1 = m_1, ..., \alpha_n = m_n) = \frac{1}{p(n)} \prod_{k=1}^{n} \binom{m_k + c(k) - 1}{m_k} \tag{1}$$

provided $\sum_{k=1}^{n} k m_k = n$, ($\mu_n(\alpha_1 = m_1, ..., \alpha_n = m_n) = 0$ otherwise). We call the vector $(\alpha_1(f), ..., \alpha_n(f))$ the type vector of $f \in \Pi_n$.

We define an associated counting function $X_n : [0,1] \times \Pi_n \to Z$ by

$$X_n(t, f) = \sum_{k=1}^{n^t} \alpha_k(f).$$

In other words, $X_n(t, f)$ equals the number of irreducible monic factors of f with degree less than or equal to n^t. Note that $X_n(1, f)$ equals the total number of factors of f. Our main result is the following theorem.

Theorem 1.1. *For $n \geq 1$, let $X_n : [0,1] \times \Pi_n \to Z$ be defined as above and suppose $Y_n : [0,1] \times \Pi_n \to R$ is defined by*

$$Y_n(t, f) = \frac{X_n(t, f) - t \log n}{\sqrt{\log n}}.$$

Then the induced measures $\mu_n \circ Y_n^{-1}$ on $D[0,1]$ converge weakly to the standard Wiener measure on $D[0,1]$ as $n \to \infty$.

The space $D[0,1]$ consists of right-continuous functions with left limits on the interval [0,1] and is endowed with the Skorohod topology. Billingsley [4] is an excellent reference on convergence of probability measures on this space. We discuss criteria for convergnece below.

Theorem 1.1 says that the process Y_n converges to standard Brownian motion on [0,1]. This result generalizes a central limit theorem obtained by Flajolet and Soria [7]. Their result follows from Theorem 1.1 by noting that $Y_n(1, \cdot) = \frac{X_n(1,\cdot) - \log n}{\sqrt{n}}$ converges in distribution to a standard normal distribution with mean 0 and variance 1. Theorem 1.1 also complements a result concerning the limiting distribution of the order statistics of the sequence $\alpha_1, \alpha_2, ..., \alpha_n$ (normalized by n) which is established in Hansen [11]. In particular, the central limit theorem says that a random polynomial of degree n has roughly $\log n$ factors, and Theorem 1.1 shows that "most" of these factors have degree on the order of n^t. On the other hand, the limiting distribution of the largest degree of the degree sequence, normalized by n, is *nondegenerate* (i.e. the largest degree in the degree sequence for a random polynomial of degree n is $O(n)$).

The statement of Theorem 1.1 is virtually the same as the statement for the Brownian motion results that have been established for random permutations by DeLaurentis and Pittel [6] and for random matrices over a finite field by Goh and Schmutz [8]. In all three cases the joint distribution for the variables which count cycles of a certain size or polynomial factors of a certain degree is equal to the joint distribution of an associated sequence of *independent* counting variables *conditioned* on a certain function of these variables. These associated sequences of variables are not the *same* in these three examples, but asymptotically each associated sequence is close (in some sense) to the same sequence of independent (but not identically distributed) Poisson variables. Shepp and Lloyd [13] were perhaps the first to use an associated sequence of counting variables to investigate the cycle structure of a random permutation, and the transform that we use in the proof given below is analogous to a transform used in their paper. The author has used similar methods (see [9] and [10]) to prove functional central limit theorems for random mappings and the Ewens sampling formula. A further investigation of the "equivalence" of the results for random polynomials and the results for random matrices is contained in Hansen and Schmutz [12].

2.Preliminaries

In order to prove Theorem 1.1, we develop a transform for computing expectations with respect to μ_n. To construct this transform we make use of an equation which relates the generating functions $P(z) = \sum_{n=0}^{\infty} p(n)z^n$ $(p(0) = 1)$ and $C(z) = \sum_{k=1}^{\infty} c(k)z^k$. It follows from (1) that

$$(1-qz)^{-1} = P(z) = \prod_{k=1}^{\infty}(1-z^k)^{-c(k)} = \exp\left(\sum_{l=1}^{\infty}\frac{C(z^l)}{l}\right). \tag{2}$$

Let $\varrho = q^{-1}$ denote the radius of convergence of $P(z)$ and $C(z)$.

Now define the auxiliary space $\Omega = \{\{m_k\} : m_k \geq 0, m_k \in Z, k \geq 1\}$ and a product measure μ_z on Ω such that for each $k \geq 1$ and $j \geq 0$,

$$\mu_z(m_k = j) = \binom{c(k)+j-1}{j}(1-(\varrho z)^k)^{c(k)}(\varrho z)^{kj}$$

where z is a parameter. Thus each coordinate of the product space Ω has a negative binomial distribution with respect to μ_z. Intuitively, a sequence $\{m_k\} \in \Omega$ can be thought to specify a type vector for a random polynomial with random degree $\nu = \sum_{k=1}^{\infty} km_k$. Of course, ν may be infinite, but if $0 < z < 1$ the random variable ν is finite a.s. with respect to μ_z and its distribution is given by the following lemma.

Lemma 2.1. *For $0 < z < 1$ and $n \geq 0$,*

$$\mu_z(\nu = n) = \frac{p(n)(\varrho z^n)}{P(\varrho z)} = z^n(1-z) \tag{3}$$

where ϱ is the radius of convergence of $P(z)$.

Proof:

Recall that $P(z) = (1-qz)^{-1}$, $p(n) = q^n$, and $\varrho = q^{-1}$, so $\frac{p(n)(\varrho z^n)}{P(\varrho z)} = z^n(1-z)$. Now compute the probability generating function for ν.

$$E(u^\nu) = \prod_{k=1}^{\infty} E(u^{km_k}) = \prod_{k=1}^{\infty}\frac{(1-(\varrho z)^k)^{c(k)}}{(1-(\varrho zu))^{c(k)}} = \frac{P(\varrho zu)}{P(\varrho z)}.$$

The last equality follows from (2). Extracting the coefficient of u^n in $E(u^\nu)$ yields (3). •

The key feature of this construction is that by conditioning on the event $\{\nu = n\}$ we can recover the joint distribution of the type vector $(\alpha_1, \alpha_2, ..., \alpha_n)$ with respect to the measure μ_n on Π_n. We state this as a lemma.

Lemma 2.2. *For $0 < z < 1$ and $n > 0$,*

$$\mu_z((m_1, m_2, ...)|\nu = n) = \mu_n(\alpha_1 = m_1, ..., \alpha_n = m_n).$$

Proof: Note that if $\nu(m_1, m_2, ...) = n$, then we must have $m_k = 0$ for all $k > n$. Hence

$$\begin{aligned}
\mu_z((m_1, m_2, ...)|\nu = n) &= \frac{\prod_{k=1}^{\infty} \binom{m_k + c(k) - 1}{m_k} (1 - (\varrho z))^{c(k)} (\varrho z)^{k m_k}}{\mu_z(\nu = n)} \\
&= \frac{P(\varrho z) \cdot \prod_{k=1}^{\infty} (1 - (\varrho z)^k)^{c(k)} \cdot \prod_{k=1}^{n} \binom{m_k + c(k) - 1}{m_k} \cdot (\varrho z)^n}{p(n)(\varrho z)^n} \\
&= \frac{1}{p(n)} \prod_{k=1}^{n} \binom{m_k + c(k) - 1}{m_k} \\
&= \mu_n(\alpha_1 = m_1, ..., \alpha_n = m_n).
\end{aligned}$$

The third equality follows from (2).•

We can use Lemma 2.2 to compute expectations with respect to μ_n in terms of expectations with respect to the product measure μ_z. Suppose that $\Psi : \Omega \to R$ and for $n \geq 1$, define functions $\Psi_n : \Pi_n \to R$ by

$$\Psi_n(f) = \Psi((\alpha_1(f), \alpha_2(f), ..., \alpha_n(f), 0, 0, ...))$$

for each $f \in \Pi_n$. Let E_z denote expectation with respect to μ_z and let E_n denote expectation with respect to μ_n on Π_n. Using Lemma 2.2., we have

$$\begin{aligned}
E_z(\Psi) &= \sum_{n=0}^{\infty} E_z(\Psi|\nu = n)\mu_z(\nu = n) \\
&= \sum_{n=1}^{\infty} E_n(\Psi_n) z^n (1 - z) + \Psi(\bar{0})(1 - z).
\end{aligned}$$

Hence

$$E_n(\Psi_n) = [z^n](1 - z)^{-1} E_z(\Psi) \tag{4}$$

where $[z^n](1 - z)^{-1} E_z(\Psi)$ denotes the coefficient of z^n in the series $(1 - z)^{-1} E_z(\Psi)$.

3. Proof of Theorem 1.1

We begin by defining a process $\bar{Y}_n$ which is "close" to $\bar{Y}_n$. For $0 \le t \le 1$ and $f \in \Pi_n$, let

$$\bar{Y}_n(t, f) = \frac{X_n(t, f) - E_n(X_n(t))}{\sqrt{\log n}}.$$

For all t and f,

$$|\bar{Y}_n(t, f) - Y_n(t, f)| = \frac{|E_n(X_n(t)) - t \log n|}{\sqrt{\log n}}.$$

Using transfrom (4), we have

$$\begin{aligned} E_n(X_n(t)) &= [z^n](1-z)^{-1} E_z\left(\sum_{k=1}^{n^t} m_k\right) \\ &= \frac{[z^n]}{(1-z)} \sum_{k=1}^{n^t} \frac{c(k)(\varrho z)^k}{(1-(\varrho z)^k)} \end{aligned}$$

and hence

$$\sum_{k=1}^{n^t} c(k)\varrho^k \le E_n(X_n(t)) \le \sum_{k=1}^{n^t} \frac{c(k)\varrho^k}{(1-\varrho^k)}.$$

It is known [3] that

$$\frac{q^k}{k}\left(1 - \frac{1}{q^{k/2}}\right) \le c(k) \le \frac{q^k}{k}.$$

Thus

$$\sum_{k=1}^{n^t} \frac{1}{k}\left(1 - \frac{1}{q^{k/2}}\right) \le E_n(X_n(t)) \le \sum_{k=1}^{n^t} \frac{1}{k}.$$

It follows that there is a constant C, independent of t and n such that

$$\sup_{t,f} |\bar{Y}_n(t, f) - Y_n(t, f)| \le \frac{C}{\sqrt{\log n}}.$$

The measures $\mu_n \circ Y_n^{-1}$ converge to Wiener measure if and only if the measures $\mu_n \circ \bar{Y}_n^{-1}$ converge to Wiener measure.

To show that the measures $\mu_n \circ \bar{Y}_n^{-1}$ converge weakly to standard Wiener measure on $D[0, 1]$ we must check that the finite-dimensional distributions associated with $\mu_n \circ \bar{Y}_n^{-1}$ converge to the finite- dimensional distributions of Wiener measure and that the sequence of measures $\mu_n \circ \bar{Y}_n^{-1}$ is tight.

Convergence of the finite-dimensional distributions

It is enough to show that for any $0 < t_1 < t_2 < ... < t_k \leq 1$, the random vector $(\bar{Y}_n(t_1), \bar{Y}_n(t_2) - \bar{Y}_n(t_1), ..., \bar{Y}_n(t_k) - \bar{Y}_n(t_{k-1}))$ converges in distribution to the random vector $(Z(t_1), Z(t_2 - t_1), ..., Z(t_k - t_{k-1}))$ where the variables $Z(t_1), Z(t_2 - t_1), ..., Z(t_k - t_{k-1}))$ are independent normal random variables with mean zero and variances $t_1, t_2 - t_1, ..., t_k - t_{k-1}$ respectively. The first step is to show that for $0 < t_1 < t_2 < ... < t_k < 1$

$$(\bar{Y}_n(t_2) - \bar{Y}_n(t_1), ..., \bar{Y}_n(t_k) - \bar{Y}_n(t_{k-1})) \to (Z(t_2 - t_1), ..., Z(t_k - t_{k-1}))$$

in distribution as $n \to \infty$. We then use a Chebyshev argument to extend this to the general case.

We give the argument in detail for the case $0 < t_1 < t_2 < t_3 < 1$. The argument can be easily generalized for any $0 < t_1 < t_2 < ... < t_k < 1$, though the notation becomes quite messy and cumbersome. Fix $0 < t_1 < t_2 < t_3 < 1$. To show that $(\bar{Y}_n(t_2) - \bar{Y}_n(t_1), \bar{Y}_n(t_3) - \bar{Y}_n(t_2))$ converges in distribution to $(Z(t_2 - t_1), Z(t_3 - t_2))$, it suffices to show (see [5], p. 335) that for any $a, b \in R$,

$$a(\bar{Y}_n(t_2) - \bar{Y}_n(t_1)) + b(\bar{Y}_n(t_3) - \bar{Y}_n(t_2)) \to aZ(t_2 - t_1) + bZ(t_3 - t_2) \tag{5}$$

in distribution as $n \to \infty$. Fix $a, b \in R$. We establish (5) by using the Method of Moments, i.e. we show that for any $r \in Z^+$,

$$\lim_{n\to\infty} E_n(a(\bar{Y}_n(t_2) - \bar{Y}_n(t_1)) + b(\bar{Y}_n(t_3) - \bar{Y}_n(t_2)))^r = E(aZ(t_2 - t_1) + bZ(t_3 - t_2))^r.$$

Fix $r \in Z^+$ and let $\xi_n = E_n(X_n(t_2) - X_n(t_1))$ and $\xi'_n = E_n(X_n(t_3) - X_n(t_2))$. Then

$$\begin{aligned} &E_n(a(\bar{Y}_n(t_2) - \bar{Y}_n(t_1)) + b(\bar{Y}_n(t_3) - \bar{Y}_n(t_2)))^r = \\ &= \sum_{k=0}^{r} \binom{r}{k} a^k b^{r-k} E_n(\bar{Y}_n(t_2) - \bar{Y}_n(t_1))^k (\bar{Y}_n(t_3) - \bar{Y}_n(t_2))^{r-k} \\ &= \frac{[z^n](1-z)^{-1}}{(\log n)^{r/2}} \sum_{k=0}^{r} a^k b^{r-k} E_z(\sum_{l>n^{t_1}}^{n^{t_2}} m_l - \xi_n)^k (\sum_{l>n^{t_2}}^{n^{t_3}} m_l - \xi'_n)^{r-k}. \end{aligned}$$

Now suppose that $0 \leq k \leq r$, then

$$E_z\left(\sum_{i>n^{t_1}}^{n^{t_2}} m_i - \xi_n)\right)^k \left(\sum_{l>n^{t_2}}^{n^{t_3}} m_i - \xi'_n\right)^{r-k} =$$

$$\sum_{j=0}^{r-k}\sum_{l=0}^{k}(-1)^{r-l-j}\binom{k}{l}\binom{r-k}{j}(\xi_n)^{(k-l)}(\xi'_n)^{(r-k-j)} E_z\left(\sum_{i>n^{t_1}}^{n^{t_2}} m_i\right)^l E_z\left(\sum_{i>n^{t_2}}^{n^{t_3}} m_i\right)^j. \tag{6}$$

This equation follows from the independence of $\sum_{i>n^{t_1}}^{n^{t_2}} m_i$ and $\sum_{i>n^{t_2}}^{n^{t_3}} m_i$ with respect to the measure P_z. Now for $0 \le l \le k$ and $0 \le j \le r-k$, write

$$E_z\left(\sum_{i>n^{t_1}}^{n^{t_2}} m_i\right)^l E_z\left(\sum_{i>n^{t_2}}^{n^{t_3}} m_i\right)^j = \sum_{i=0}^{\infty} a_i(l,j,n)z^i = f_{l,j,n}(z).$$

It is straightforward to verify that the coefficients $a_i(l,j,n)$ are non- negative. Observe that

$$f_{l,j,n}(1) = E\left(\sum_{i>n^{t_1}}^{n^{t_2}} \tilde{m}_i\right)^l \left(\sum_{i>n^{t_2}}^{n^{t_3}} \tilde{m}_i\right)^j$$

where $\tilde{m}_1, \tilde{m}_2, ...$ is a sequence of independent random variables defined on a common probability space such that $\tilde{m}_k$ is negative binomial with $P(\tilde{m}_k = j) = \binom{j+c(k)-1}{j}(1-\varrho^k)^{c(k)}\varrho^{kj}$ for $j \ge 0$. We show that

$$|[z^n](1-z)^{-1}f_{l,j,n}(z) - f_{l,j,n}(1)| = \sum_{i>n} a_i(l,j,n) = O(n^{2j+2l}\varrho^{n/2}) \tag{7}$$

from which it follows that

$$\begin{aligned}
&\lim_{n\to\infty}[z^n]\frac{(1-z)^{-1}}{(\log n)^{r/2}}E_z\left(\sum_{i>n^{t_1}}^{n^{t_2}} m_i - \xi_n\right)^k \left(\sum_{i>n^{t_2}}^{n^{t_3}} m_i - \xi'_n\right)^{r-k} \\
&= \lim_{n\to\infty}(\log n)^{-r/2}E\left(\sum_{i>n^{t_1}}^{n^{t_2}} \tilde{m}_i - \xi_n\right)^k \left(\sum_{i>n^{t_2}}^{n^{t_3}} \tilde{m}_i - \xi'_n\right)^{r-k} \\
&= E(Z(t_2-t_1))^k E(Z(t_3-t_2))^{r-k}.
\end{aligned} \tag{8}$$

The last equality on the right side of (8) follows from the convergence of the moments of the sums $\sum_{n^{t_1}}^{n^{t_2}} \tilde{m}_i$ and $\sum_{n^{t_2}}^{n^{t_3}} \tilde{m}_i$ (when normalized). to the moments of $Z(t_2-t_1)$ and $Z(t_3-t_2)$ respectively. To establish (7), we expand $\left(\sum_{i>n^{t_1}}^{n^{t_2}} m_i\right)^l \left(\sum_{i>n^{t_2}}^{n^{t_3}} m_i\right)^j$. This yields no more than n^{j+l} terms of the form $m_{i_1}m_{i_2}...m_{i_{j+l}}$ (indices need not be distinct). It suffices to show that

$$|[z^n](1-z)^{-1}E_z(m_{i_1}\cdots m_{i_{j+l}}) - E(\tilde{m}_{i_1},\cdots\tilde{m}_{i_{j+l}})| = O(n^{j+l}\varrho^{n/2}) \tag{9}$$

for each term $m_{i_1}\cdots m_{i_{j+l}}$ in the expansion of $\left(\sum_{i>n^{t_1}}^{n^{t_2}} m_i\right)^l \left(\sum_{i>n^{t_2}}^{n^{t_3}} m_i\right)^j$. We outline the proof of (9) for one case. The general case follows by a similar argument, though messier to write down. Consider $E_z((m_{i_1})^l(m_{i_2})^j)$ where $n^{t_1} < i_1 \le n^{t_2}$ and $n^{t_2} < i_2 \le n^{t_3}$. It can be verified that

$$E_z(m_{i_1})^l = \sum_{s=1}^{l} \alpha_s \frac{[c(i_1)]^s(\varrho z)^{i_1 s}}{(1-(\varrho z)^i)^s}$$

$$E_z(m_{i_2})^j = \sum_{s'=1}^{j} \beta_{s'} \frac{[c(i_2)]^{s'}(\varrho z)^{i_2 s'}}{(1-(\varrho z)^{i_2})^{s'}}$$

where the α's and β's are non-negative coefficients and $[c]^s = c(c+1)\cdots(c+s-1)$. Since

$$\frac{q^d}{d}\left(1-q^{-d/2}\right) \le c(d) \le \frac{q^d}{d}$$

there exist a constant C, which may depend on j and l but does not depend on n, such that $[c(d)]^k \varrho^{dk} \le \frac{C}{d}$ for all $k \le l \vee j$. Now fix $1 \le s \le l$ and $1 \le s' \le j$, then for $m \ge i_1 s + i_2 s'$,

$$\begin{aligned}
&[z^m]\frac{[c(i_1)]^s[c(i_2)]^{s'}(\varrho z)^{i_1 s + i_2 s'}}{(1-(\varrho z)^{i_1})^s(1-(\varrho z)^{i_2})^{s'}} \\
&\le \left(\frac{C}{i_1}\right)^s \left(\frac{C}{i_2}\right)^{s'} [z^{m'}](1-(\varrho z))^{-s-s'} \\
&= \left(\frac{C}{i_1}\right)^s \left(\frac{C}{i_2}\right)^{s'} \binom{m'+s+s'-1}{m'} \varrho^{m'} \\
&\le (C)^{s+s'}(m')^{s+s'}\varrho^{m'}
\end{aligned} \tag{10}$$

where $m' = m - i_1 s - i_2 s'$. Hence for all large n,

$$\begin{aligned}
&\left| [z^n](1-z)^{-1}\frac{[c(i_1)]^s[c(i_2)]^{s'}(\varrho z)^{i_1 s + i_2 s'}}{(1-(\varrho z)^{i_1})^s(1-(\varrho z)^{i_2})^{s'}} - \frac{[c(i_1)]^s[c(i_2)]^{s'}\varrho^{i_1 s + i_2 s'}}{(1-\varrho^{i_1})^s(1-\varrho^{i_2})^{s'}} \right| \\
&= \sum_{m>n} [z^m]\frac{[c(i_1)]^s[c(i_2)]^{s'}(\varrho z)^{i_1 s + i_2 s'}}{(1-(\varrho z)^{i_1})^s(1-(\varrho z)^{i_2})^{s'}} \\
&\le \sum_{m'>n-i_1 s - i_2 s'} (C)^{s+s'}(m')^{s+s'}(\varrho)^{m'} \\
&\le (C)^{s+s'}(n-i_1 s - i_2 s')^{s+s'}\varrho^{n-i_1 s - i_2 s'}\sum_{k=0}^{\infty}(1+k)^{s+s'}\varrho^k \\
&\le (C)^{s+s'} n^{s+s'} \varrho^{n/2}\sum_{k=0}^{\infty}(1+k)^{2r}\varrho^k
\end{aligned} \tag{11}$$

since $n - i_1 s - i_2 s' \ge n/2$ for all sufficiently large n. Therefore, summing (11) over $1 \le s \le l$ and $1 \le s' \le j$, we have

$$|[z^n](1-z)^{-1}E_z(m_{i_1})^l E_z(m_{i_2})^j - E(\tilde{m}_{i_1})^l(\tilde{m}_{i_2})^j| = O(n^{j+l}\varrho^{n/2})$$

and by a similar argument (9) holds in all cases. Equation (7) now follows from (9) and the fact that there are less than n^{j+l} terms in the expansion of $\left(\sum_{i>n^{t_1}}^{n^{t_2}} m_i\right)^l \left(\sum_{i>n^{t_2}}^{n^{t_3}} m_i\right)^j$.

Chebyshev bounds

To complete the proof that the finite-dimensional distributions converge, we need the bounds

$$P(|\bar{Y}_n(\epsilon)| > \sqrt[4]{\epsilon}) \leq \frac{2\sqrt{\epsilon}}{(1-\varrho)^2} \tag{12i}$$

$$P(|\bar{Y}_n(1) - \bar{Y}_n(1-\epsilon)| > \sqrt[4]{\epsilon}) \leq \frac{2\sqrt{\epsilon}}{(1-\varrho)^2} \tag{12ii}$$

for all large n. By Chebyshev's inequality

$$P(|\bar{Y}_n(\epsilon)| > \sqrt[4]{\epsilon}) \leq \frac{E_n(X_n(\epsilon) - E_n(X_n(\epsilon)))^2}{\sqrt{\epsilon}\log n}.$$

Let $\delta_n(j) = E_n(\alpha_j) = \frac{[z^n]}{(1-z)} E_z(m_j)$, then

$$\begin{aligned}
\frac{E_n(X_n(\epsilon) - E_n(X_n(\epsilon)))^2}{\log n} &= \frac{[z^n](1-z)^{-1}}{\log n} E_z\Big(\sum_{k=1}^{n^\epsilon} m_k - \sum_{k=1}^{n^\epsilon} \delta_n(k)\Big)^2 \\
&= \frac{[z^n](1-z)^{-1}}{\log n}\left[E_z\Big(\sum_{k=1}^{n^\epsilon} m_k - E_z(m_k)\Big)^2 + \Big(\sum_{k=1}^{n^\epsilon} E_z(m_k) - \delta_n(k)\Big)^2\right] \\
&= \frac{[z^n](1-z)^{-1}}{\log n} \sum_{k=1}^{n^\epsilon} \frac{c(k)(\varrho z)^k}{(1-(\varrho z)^k)^2} \\
&+ \frac{[z^n](1-z)^{-1}}{\log n}\left[\Big(\sum_{k=1}^{n^\epsilon} E_z(m_k)\Big)^2 - \sum_{k=1}^{n^\epsilon} E_z(m_k) \cdot \sum_{j=1}^{n^\epsilon} \delta_n(j)\right] \\
&+ \frac{[z^n](1-z)^{-1}}{\log n}\left[\Big(\sum_{k=1}^{n^\epsilon} \delta_n(j)\Big)^2 - \sum_{k=1}^{n^\epsilon} E_z(m_k) \cdot \sum_{j=1}^{n^\epsilon} \delta_n(j)\right].
\end{aligned} \tag{13}$$

The last term on the right side of (13) is zero, so it remains to bound the other terms. For all large n, the first term on the right side of (13) is bounded by

$$(\log n)^{-1} \sum_{k=1}^{n^\epsilon} \frac{c(k)\varrho^k}{(1-\varrho^k)^2} \leq \frac{(\log n)^{-1}}{(1-\varrho)^2} \sum_{k=1}^{n^\epsilon} \frac{1}{k} \leq \frac{2\epsilon}{(1-\varrho)^2}.$$

Next, let $B(z) = \sum_{k=1}^{n^\epsilon} E_z(m_k) = \sum_{k=1}^{\infty} \beta_k z^k$ and note that $\sum_{k=1}^{n} \beta_k = \frac{[z^n]}{(1-z)} B(z) = \sum_{j=1}^{n^\epsilon} \delta_n(j)$. Also, the coefficients of $B(z)$ are positive. Hence

$$\frac{[z^n]}{(1-z)}\left(\Big(\sum_{k=1}^{n^\epsilon} E_z(m_k)\Big)^2 - \sum_{k=1}^{n^\epsilon} E_z(m_k) \cdot \sum_{j=1}^{n^\epsilon} \delta_n(j)\right) = \sum_{k=1}^{n} \beta_k \sum_{j=1}^{n-k} \beta_j - \Big(\sum_{k=1}^{n} \beta_k\Big)^2 \leq 0.$$

This establishes (12i). Similar calculations establish the second bound (12ii).

We now show convergence of the finite-dimensional distributions in the two remaining cases. First, suppose that $0 < t_1 < t_2 < ... < t_k < 1$ and $a_1, ..., a_k \in R$ then

$$P(\bar{Y}_n(t_1) \leq a_1, \bar{Y}_n(t_2) - \bar{Y}_n(1) \leq a_2, ..., \bar{Y}_n(t_k) - \bar{Y}_n(t_{k-1}) \leq a_k)$$

$$\leq P(\bar{Y}_n(t_1) - \bar{Y}_n(\epsilon) \leq a_1 + \sqrt[4]{\epsilon}, \bar{Y}_n(t_2) - \bar{Y}_n(t_1) \leq a_2, .., \bar{Y}_n(t_k) - \bar{Y}_n(t_{k-1}) \leq a_k) + P(|\bar{Y}_n(\epsilon)| > \sqrt[4]{\epsilon}).$$

Hence

$$\limsup_n P(\bar{Y}_n(t_1) \leq a_1, \bar{Y}_n(t_2) - \bar{Y}_n(t_1) \leq a_2, ..., \bar{Y}_n(t_k) - \bar{Y}_n(t_{k-1}) \leq a_{k-1})$$

$$\leq P(Z(t_1 - \epsilon) \leq a_1 + \sqrt[4]{\epsilon}, Z(t_2 - t_1) \leq a_2, ...Z(t_k - t_{k-1}) \leq a_k) + \frac{2\sqrt{\epsilon}}{(1-\varrho)^2} \tag{14}$$

where $Z(t_1 - \epsilon), ..., Z(t_k - t_{k-1})$ are independent, mean zero, Gaussian variables with variances $t_1 - \epsilon, t_2 - t_1, ..., t_k - t_{k-1}$ respectively. Let $\epsilon \to 0$ on both sides of (14) to obtain

$$\limsup_n P(\bar{Y}_n(t_1) \leq a_1, ..., \bar{Y}_n(t_k) - \bar{Y}_n(t_{k-1}) \leq a_k) \leq P(Z(t_1) \leq a_1, ..., Z(t_k - t_{k-1}) \leq a_k).$$

Similarly,

$$\liminf_n P(\bar{Y}_n(t_1) \leq a_1, ..., \bar{Y}_n(t_k) - \bar{Y}_n(t_{k-1}) \leq a_k) \geq P(Z(t_1) \leq a_1, ..., Z(t_k - t_{k-1}) \leq a_k)$$

since

$$P(\bar{Y}_n(t_1) \leq a_1, \bar{Y}_n(t_2) - \bar{Y}_n(t_1) \leq a_2, ..., \bar{Y}_n(t_k) - \bar{Y}_n(t_{k-1}) \leq a_k)$$

$$\geq P(\bar{Y}_n(t_1) - \bar{Y}_n(\epsilon) \leq a_1 - \sqrt[4]{\epsilon}, \bar{Y}_n(t_2) - \bar{Y}_n(t_1) \leq a_2, ..., \bar{Y}_n(t_k) - \bar{Y}_n(t_{k-1}) \leq a_k) - P(|\bar{Y}_n(\epsilon)| > \sqrt[4]{\epsilon}).$$

This establishes convergence in distribution in the first case.

In the case $0 \leq t_1 < t_2 < ... < t_k = 1$ arguments similar to those given above (employing the second Chebyshev bound in this case) yield

$$\lim_{n\to\infty} P(\bar{Y}_n(t_1) \leq a_1 \bar{Y}_n(t_2) - \bar{Y}_n(t_1) \leq a_2, ..., \bar{Y}_n(1) - \bar{Y}_n(t_{k-1}) \leq a_k)$$

$$= P(Z(t_1) \leq a_1, ..., Z(1) - Z(t_{k-1}) \leq a_k).$$

Tightness

It suffices to show (see Billingsley [4] p.128) that there exists a constant $C > 0$ such that for every $n > 0$ and all $0 \leq t_1 < t < t_2 \leq 1$,

$$E_n(\bar{Y}_n(t_2) - \bar{Y}_n(t))^2(\bar{Y}_n(t) - \bar{Y}_n(t_1))^2 \leq C(t_2 - t_1)^2.$$

We note that there are two cases where $E_n(\bar{Y}_n(t_2)-\bar{Y}_n(t))^2(\bar{Y}_n(t)-\bar{Y}_n(t_1))^2=0$. First, if $\log(k-1)/\log n \le t_1 \le t < \log k/\log n$ for some $2\le k\le n$ then $\bar{Y}_n(t)\equiv \bar{Y}_n(t_1)$ and the expectation is 0. Likewise, if $\log(k-1)/\log n \le t \le t_2 < \log k/\log n$ for some $2\le k\le n$ then $\bar{Y}_n(t)\equiv\bar{Y}_n(t_2)$ and the expectation is 0. The expectation will be nonzero only if $\log(k-1)/\log n\le t_1<\log k/\log n$ and $\log(k+1)/\log n\le t_2$ for some $2\le k\le n-1$. Thus, to avoid trivialities, we assume that

$$t_2-t_1 \ge \frac{\log(k+1)-\log k}{\log n} \ge \frac{1}{k\log n} \ge \frac{1}{2n^{t_1}\log n}$$

for some $2\le k\le n-1$.

Fix $n>0$.

$$\begin{aligned}
&E_n(\bar{Y}_n(t_2)-\bar{Y}_n(t))^2(\bar{Y}_n(t)-\bar{Y}_n(t_1))^2\\
&=\frac{[z^n]}{(1-z)(\log n)^2}E_z(\bar{Y}_n(t_2)-\bar{Y}_n(t))^2(\bar{Y}_n(t)-\bar{Y}_n(t_1))^2\\
&=\frac{[z^n]}{(1-z)(\log n)^2}\left[Var_z(\sum_{k>n^{t_1}}^{n^t} m_k)+(\Gamma(z)-\Gamma)^2\right]\cdot\left[Var_z(\sum_{j>n^t}^{n^{t_2}} m_j)+(\tilde\Gamma(z)-\tilde\Gamma)^2\right]
\end{aligned} \tag{15}$$

where $\Gamma(z)=\sum_{k>n^{t_1}}^{n^t}E_z(m_k)=\sum_{i=1}^\infty \gamma_i z^i$, $\Gamma=\frac{[z^n]}{(1-z)}\Gamma(z)=\sum_{k=1}^n\gamma_k=E_n(X_n(t_2)-X_n(t))$, $\tilde\Gamma(z)=\sum_{k>n^t}^{n^{t_2}}\tilde\gamma_k z^k$, and $\tilde\Gamma=\frac{[z^n]}{(1-z)}\tilde\Gamma(z)=\sum_{i=1}^n\tilde\gamma_i=E_n(X_n(t)-X_n(t_1))$. The coefficients of $\Gamma(z)$ and $\tilde\Gamma(z)$ are positive. We proceed to bound the right side of (15).

First,

$$\begin{aligned}
&\frac{[z^n]}{(\log n)^2(1-z)}Var_z(\sum_{k>n^{t_1}}^{n^t}m_k)Var_z(\sum_{j>n^t}^{n^{t_2}}m_j)\\
&=\frac{[z^n]}{(\log n)^2(1-z)}\sum_{k>n^{t_1}}^{n^t}\frac{c(k)\varrho^k z^k}{(1-(\varrho z)^k)^2}\cdot\sum_{j>n^t}^{n^{t_2}}\frac{c(j)\varrho^j z^j}{(1-(\varrho z)^j)^2}\\
&\le\frac{1}{(\log n)^2}\frac{1}{(1-\varrho)^2}\sum_{k>n^{t_1}}^{n^t}\frac{1}{k}\cdot\sum_{j>n^t}^{n^{t_2}}\frac{1}{j}\\
&\le c_1(t_2-t_1)^2
\end{aligned}$$

where c_1 is a constant that can be chosen independently of n.

Next consider

$$\frac{[z^n]}{(\log n)^2(1-z)}Var_z(\sum_{k>n^{t_1}}^{n^t}m_k)(\tilde\Gamma(z)-\tilde\Gamma)^2$$

$$=\frac{[z^n]}{(\log n)^2(1-z)}Var_z(\sum_{k>n^{t_1}}^{n^t}m_k)(\tilde\Gamma^2(z)-\tilde\Gamma(z)\cdot\tilde\Gamma)+\frac{[z^n]}{(\log n)^2(1-z)}Var_z(\sum_{k>n^{t_1}}^{n^t}m_k)(\tilde\Gamma^2-\tilde\Gamma(z)\cdot\tilde\Gamma).$$

Let $\Phi(z) = Var_z(\sum_{k>n^{t_1}}^{n^t} m_k)\tilde{\Gamma}(z) = \sum_{k=1}^{\infty} \phi_k z^k$ (all $\phi_k \geq 0$). Then

$$\begin{aligned}
\frac{[z^n]}{(1-z)} Var_z(\sum_{k>n^{t_1}}^{n^t} m_k)(\tilde{\Gamma}^2(z) - \tilde{\Gamma}(z)\cdot\tilde{\Gamma}) &= \frac{[z^n]}{(1-z)}(\Phi(z)\tilde{\Gamma}(z) - \Phi(z)\tilde{\Gamma}) \\
&= \sum_{k=1}^{n} \phi_k \sum_{j=1}^{n-k} \gamma_j - \sum_{k=1}^{n}\sum_{j=1}^{n} \phi_k \gamma_j \\
&\leq 0
\end{aligned}$$

On the other hand,

$$\begin{aligned}
&\frac{[z^n]}{(\log n)^2(1-z)} Var_z(\sum_{k>n^{t_1}}^{n^t} m_k)(\tilde{\Gamma}^2 - \tilde{\Gamma}(z)\cdot\tilde{\Gamma}) \\
&\leq \frac{\tilde{\Gamma}}{(\log n)^2}\left(\frac{[z^n]}{(1-z)}\left[Var_z(\sum_{k>n^{t_1}}^{n^t} m_k)\sum_{j>n^t}^{n^{t_2}} \frac{c(j)\varrho^j}{(1-\varrho^j)}\right] - \frac{[z^n]}{(1-z)}\left[Var_z(\sum_{k>n^{t_1}}^{n^t} m_k)\sum_{j>n^t}^{n^{t_2}} c(j)\varrho^j z^j\right]\right) \\
&\leq \frac{\tilde{\Gamma}(1)}{(\log n)^2}\sum_{k>n^{t_1}}^{n^t} \frac{[z^n]}{(1-z)}\frac{c(k)\varrho^k z^k}{(1-(\varrho z)^k)^2}\left(\sum_{j>n^t}^{n^{t_2}}\frac{c(j)\varrho^j}{1-\varrho^j} - \sum_{j>n^t}^{n^{t_2}} c(j)\varrho^j z^j\right) \\
&\leq \frac{\tilde{\Gamma}(1)}{(\log n)^2}\sum_{k>n^{t_1}}^{n^t} \frac{[z^n]}{(1-z)} c(k)\varrho^k z^k\left(\sum_{j>n^t}^{n^{t_2}}\frac{c(j)\varrho^j}{(1-\varrho^j)} - \sum_{j>n^t}^{n^{t_2}} c(j)\varrho^j z^j\right) \\
&+ \frac{\tilde{\Gamma}(1)}{(\log n)^2}\sum_{k>n^{t_1}}^{n^t} c(k)\varrho^k\left(\frac{1}{(1-\varrho^k)^2} - 1\right)\cdot\sum_{j>n^t}^{n^{t_2}}\frac{c(j)\varrho^j}{1-\varrho^j}.
\end{aligned} \tag{16}$$

The second term on the right side of (16) is bounded by

$$\frac{1}{(\log n)^2}\left(\frac{1}{(1-\varrho)}\sum_{m>n^t}^{n^{t_2}}\frac{1}{m}\right)\left(\sum_{k=1}^{\infty}\frac{1}{k}\left(\frac{1}{(1-\varrho^k)^2} - 1\right)\right)\left(\frac{1}{(1-\varrho)}\sum_{j>n^t}^{n^{t_2}}\frac{1}{j}\right) \leq c_2(t_2 - t_1)^2$$

for some positive constant c_2 which does not depend on n , but which may depend on ϱ.

It remains to bound the first term on the right side of (16). For $k < n/2$,

$$\begin{aligned}
&\frac{[z^n]}{(1-z)} c(k)\varrho^k z^k\left(\sum_{j>n^t}^{n^{t_2}}\frac{c(j)\varrho^j}{(1-\varrho^j)} - \sum_{j>n^t}^{n^{t_2}} c(j)\varrho^j z^j\right) \\
&\leq c(k)\varrho^k\left(\sum_{j>n^t}^{n^{t_2}\wedge n-k} c(j)\varrho^j\left(\frac{1}{1-\varrho^j} - 1\right) + \sum_{j>n/2}^{n}\frac{c(j)\varrho^j}{1-\varrho^j}\right) \\
&\leq \frac{1}{k}\left(\sum_{j>n^t}^{n^{t_2}}\frac{1}{j}\left(\frac{1}{1-\varrho^j} - 1\right) + \sum_{j>n/2}^{n}\frac{1}{j}\frac{1}{1-\varrho^j}\right) \\
&\leq \frac{c_3}{k}
\end{aligned}$$

for some positive constant c_3 which does not depend on n. For $k \geq n/2$,

$$\frac{[z^n]}{(1-z)} c(k)\varrho^k z^k \left(\sum_{j>n^t}^{n^{t_2}} \frac{c(j)\varrho^j}{1-\varrho^j} - \sum_{j>n^t}^{n^{t_2}} c(j)\varrho^j z^j \right)$$

$$\leq \frac{2}{n(1-\varrho)} \sum_{j>n^t}^{n^{t_2}} \frac{1}{j}.$$

Hence the first term on the right side of (16) is bounded above by

$$\frac{\tilde{\Gamma}(1)}{(\log n)^2} \left(\sum_{k>n^{t_1}}^{n^t \wedge n/2} \frac{c_3}{k} + \frac{2}{n(1-\varrho)} \sum_{j>n^t}^{n^{t_2}} \frac{1}{j} \right)$$

$$\leq c_4(t_2 - t_1)^2$$

for some positive constant c_4 which is independent of n (since $\tilde{\Gamma}(1) \leq (1-\varrho)^{-1} \sum_{n^t}^{n^{t_2}} \frac{1}{k}$). Similar calculations establish that

$$\frac{[z^n]}{(1-z)(\log n)^2} Var_z(\sum_{k>n^t}^{n^{t_2}} m_k)(\Gamma^2(z) - 2\Gamma(z) \cdot \Gamma + \Gamma^2) \leq c_5(t_2 - t_1)^2$$

for some positive constant c_5 which is independent of n.

Finally, we bound

$$\frac{[z^n]}{(1-z)(\log n)^2} (\Gamma(z) - \Gamma)^2 (\tilde{\Gamma}(z) - \tilde{\Gamma})^2$$

$$= \frac{[z^n]}{(1-z)(\log n)^2} (\Gamma^2(z) - 2\Gamma(z) \cdot \Gamma + \Gamma^2)(\tilde{\Gamma}(z) - \tilde{\Gamma})^2. \tag{17}$$

First, by calculations similar to those made above,

$$\frac{\Gamma^2 [z^n]}{(1-z)(\log n)^2} (\tilde{\Gamma}^2(z) - 2\tilde{\Gamma}(z) \cdot \tilde{\Gamma} + \tilde{\Gamma}^2)$$

$$= \frac{\Gamma^2}{(\log n)^2} \frac{[z^n]}{(1-z)} (\tilde{\Gamma}^2(z) - \tilde{\Gamma}(z) \cdot \tilde{\Gamma})$$
$$\leq 0.$$

Next,

$$\frac{-2\Gamma}{(\log n)^2} \frac{[z^n]}{(1-z)} \Gamma(z) (\tilde{\Gamma}(z) - \tilde{\Gamma})^2$$

$$= \frac{2\Gamma \cdot \tilde{\Gamma}}{(\log n)^2} \frac{[z^n]}{(1-z)} (\Gamma(z)\tilde{\Gamma}(z) - \Gamma(z)\tilde{\Gamma}) + \frac{2\Gamma}{(\log n)^2} \frac{[z^n]\Gamma(z)}{(1-z)} (\tilde{\Gamma}(z) \cdot \tilde{\Gamma} - \tilde{\Gamma}^2(z)) \tag{18}$$

The first term on the right side of (18) is less than 0, so it remains to bound the second term. First note that there exists a positive constant $\hat{C}$, independent of n, such that for $k \geq 1$, $\gamma_k < \hat{C}/k$ and $\tilde{\gamma}_k < \hat{C}/k$. Now consider

$$\frac{2\Gamma[z^n]}{(\log n)^2(1-z)}\Gamma(z)(\tilde{\Gamma}(z)\cdot\tilde{\Gamma} - \tilde{\Gamma}^2(z)) = \frac{2\Gamma}{(\log n)^2}\sum_{k=1}^{n}\gamma_k d_{n-k}$$

where

$$\begin{aligned} d_{n-k} &= \frac{[z^{n-k}]}{(1-z)}(\tilde{\Gamma}(z)\cdot\tilde{\Gamma} - \tilde{\Gamma}^2(z)) \\ &= \sum_{j=1}^{n-k}\tilde{\gamma}_j\sum_{m=1}^{n}\tilde{\gamma}_m - \sum_{j=1}^{n-k}\tilde{\gamma}_j\sum_{m=1}^{n-k-j}\tilde{\gamma}_m \\ &= \sum_{j=1}^{n-k}\tilde{\gamma}_j\sum_{m>(n-k-j)}^{n}\tilde{\gamma}_m \\ &\leq \sum_{j=1}^{n-k-1}\tilde{\gamma}_j\sum_{m>n-k-j}^{n}\tilde{\gamma}_m + \frac{\hat{C}}{n-k}\tilde{\Gamma}. \end{aligned}$$

Hence,

$$\frac{2\Gamma}{(\log n)^2}\sum_{k=1}^{n}\gamma_k\cdot d_{n-k}$$

$$\leq \frac{2\Gamma}{(\log n)^2}\sum_{k=1}^{n}\gamma_k\sum_{j=1}^{n-k-1}\tilde{\gamma}_j\sum_{m>n-k-j}^{n}\tilde{\gamma}_m + \frac{2\Gamma\tilde{\Gamma}}{(\log n)^2}\sum_{k=1}^{n}\frac{\hat{C}}{k}\frac{\hat{C}}{n-k}. \tag{19}$$

The second term on the right side of (19) is bounded by $c_6(t_2-t_1)^2$ for some positive constant which is independent of n since

$$\frac{\Gamma\tilde{\Gamma}}{(\log n)^2} \leq \frac{1}{(\log n)^2}\frac{1}{(1-\varrho)^2}\sum_{k>n^{t_1}}^{n^t}\frac{1}{k}\sum_{j>n^t}^{n^{t_2}}\frac{1}{j}.$$

Since $\gamma_k \leq \hat{C}/k$ and $\tilde{\gamma}_k \leq \hat{C}/k$, the first term is bounded by

$$\frac{8\Gamma\hat{C}^2}{(\log n)^2}\sum_{j=1}^{n}\tilde{\gamma}_j\sum_{k>n/4}^{n-j-1}\frac{\log(\frac{n}{n-k-j})}{n} + \frac{8\Gamma\hat{C}^2}{(\log n)^2}\sum_{k=1}^{n}\gamma_k\sum_{j>n/4}^{n-k-1}\frac{\log(\frac{n}{n-k-j})}{n}$$

$$+\frac{2\Gamma}{(\log n)^2}\sum\sum_{k+j\leq n/2}\gamma_k\tilde{\gamma}_j\cdot(\hat{C}\log(\frac{n}{n-j-k}))$$

$$\leq \left(\frac{8\hat{C}^2\Gamma\tilde{\Gamma}}{(\log n)^2} + \frac{8\hat{C}^2\Gamma^2}{(\log n)^2}\right)\left(-\int_0^1\log(1-x)dx\right) + \frac{4\Gamma\hat{C}}{(\log n)^2}\sum\sum_{k+j<n/2}\gamma_k\cdot\tilde{\gamma}_j\left(\frac{k}{n}+\frac{j}{n}\right)$$

$$\leq c_7(t_2-t_1)^2 \tag{20}$$

where c_7 is a positive constant (independent of n). This establishes the bound for (17).

Finally,

$$\frac{[z^n]}{(\log n)^2(1-z)}\Gamma^2(z)(\tilde{\Gamma}(z)-\tilde{\Gamma})^2$$

$$= \frac{[z^n]}{(\log n)^2(1-z)}(\Gamma^2(z)\tilde{\Gamma}^2(z)-\Gamma^2(z)\tilde{\Gamma}(z)\tilde{\Gamma}) + \frac{\tilde{\Gamma}}{(\log n)^2}\frac{[z^n]}{(1-z)}(\Gamma^2(z)\tilde{\Gamma}-\Gamma^2(z)\tilde{\Gamma}(z)). \tag{21}$$

By calculations similar to those made above, it is easy to see that the first term on the right side of (21) is less than zero, and calculations similar to those used to obtain (20) establish that the second term is bounded by $c_8(t_2-t_1)^2$ where c_8 is a positive constant which is independent of n. We add the bounds that we have obtained to establish

$$E_n(\bar{Y}_n(t_2)-\bar{Y}_n(t))^2(\bar{Y}_n(t)-\bar{Y}_n(t_1))^2 \le C(t_2-t_1)^2$$

where C is a positive constant which does not depend on n. This completes the proof of the theorem.•

Author's Note: While preparing this paper I have recently learned that this result has been independently (and simultaneously) obtained by Arratia, Barbour, and Tavare [1] using methods which are quite different than the methods used above. Their method involves comparing the counting variables $\alpha_1, \alpha_2, ...$ to a sequence of independent variables via a coupling of the sequences on the same probability space. Using this method they are also able to obtain a bound on the rate of convergence of $O(\log\log n/\sqrt{\log n})$. Similar calculations for random permutations, the Ewens sampling formula, and random mappings are contained in [2].

References.

[1] Arratia, R., Barbour, A.D., and Tavare, S. *On random polynomials over finite fields.* Math. Proc. Camb. Phil. Soc., in press. (1992).

[2] Arratia, R. and Tavare, S. *Limit Theorems for combinatorial structures via discrete process approximations.* Rand. Struc. Alg., **3** (1992) 321-345.

[3] Berlekamp, E. Algebraic Coding Theory, 2^{nd} ed. Aegean Park Press. (1984).

[4] Billingsley, P. Convergence of probability measures. Wiley, NY. (1976).

[5] Billingsley, P. Probability and Measure. Wiley, NY. (1979).

[6] DeLaurentis, J.M. and Pittel, B. *Random permutations and Brownian motion*, Pacific J. Math., **119** (1985) 287-301.

[7] Flajolet, P. and Soria, M. *Gaussian limiting distributions for the number of components in combinatorial structures*, Jour. Comb. Theor. A. **153** (1990) 165-182.

[8] Goh, W. and Schmutz, E. *Random matrices and Brownian motion.* To appear in Combinatorics, Probability and Computing. (1993).

[9] Hansen, J.C. *A functional central limit theorem for random mappings.* Ann. Probab. **17** (1989) 317-332.

[10] Hansen, J.C. *A functional central limit theorem for the Ewens sampling formula.* J. Appl. Prob. **27** (1990) 28-47.

[11] Hansen, J.C. *Order statistics for decomposable combinatorial structures.* To appear in Rand. Struc. Alg., (1993).

[12] Hansen, J.C. and Schmutz, E. *How random is the characteristic polynomial of a random matrix?* To appear in Math. Proc. Camb. Phil. Soc., (1993).

[13] Shepp, L.A. and Lloyd, S.P. *Ordered cylce lenghts in a random permutation.* Trans. Amer. Math. Soc. **121** (1966) 340-357.