ON STRAIGHT SELECTION SORT

Andrew Chi-Chih Yao

CS-TR-185-88

October 1988

On Straight Selection Sort [1]

Andrew Chi-Chih Yao

Department of Computer Science
Princeton University
Princeton, New Jersey 08544

Abstract

The expected value of $B_n = B'_n - (n-1)$, where B'_n is the number of right-to-left maxima encountered by the straight selection sort, is well known to be $(n+1)H_n - 2n$, but the variance of B_n has remained unanalyzed. In this paper, we derive an exact formula for the variance of B_n, and show that it is asymptotically equal to $\alpha\, n^{3/2}(1 + o(1))$, where $\alpha > 0$ is an explicitly defined constant.

[1] This research was supported in part by the National Science Foundation under Grant No. CCR-8818283.

1 Introduction

The study of the average-case behavior of sorting algorithms is a major topic in the *Mathematical Analysis of Algorithms*, an area first pioneered by Knuth [K1-3]. (See Greene and Knuth [GK], Flajolet and Sedgewick [FS], and Flajolet and Vitter [FV] for more recent surveys of this area.) Although there have been a multitude of interesting results regarding algorithms for sorting [K3] (also see e.g. [S] [Y]), many questions concerning sorting algorithms remain open. In this paper, we will answer one such question concerning a classical sorting algorithm, known as the *straight selection sort*.

Given an array $A[1:n]$ of distinct integers, a sorting algorithm will permute the contents of A such that the integers are in ascending order in the array. In *straight selection sort* (see Knuth [K3, Section 5.2.3]), this is accomplished in $n-1$ phases. Before the start of the j-th phase, $1 \leq j < n$, the $j-1$ largest elements in A will be in their final positions, namely, $A[n]$, $A[n-1]$, $\ldots$, $A[n-j+2]$; during phase j, the largest element in the subarray $A[1:n-j+1]$ will be identified and exchanged with the element currently in $A[n-j+1]$. The array A will be sorted after $n-1$ phases.

Suppose that the array A contains initially a random permutation of n distinct integers. One quantity of interest in the analysis of the performance is B_n, the number of times the register holding the temporary maxima needs to be updated (see [K3]). One can write $B_n = \sum_{1\leq j<n}(C_{n,j}-1)$, where $C_{n,j}$ is the number of right-to-left maxima[2] in $A[1\colon n-j+1]$ at the start of phase j. The expected value of B_n is well known to be $(n+1)H_n - 2n$, where H_n is the Harmonic number $\sum_{1\leq j\leq n}(1/j)$, but the variance of B_n has not been analyzed (see Knuth [K3, exercise 5.2.3 - 7]). In this paper we will give an exact formula for $Var(B_n)$, and an asymptotic expression for large n.

An essential step in the derivation is to relate $Var(B_n)$ to a geometric stochastic process, which is simpler to analyze. Let $N > 0$ be any integer. Let $S = \{(x_i, y_i) \mid 1 \leq i \leq N\}$, where x_i are N distinct real numbers, and y_i are N distinct real numbers. We call such an S a *standard N-set*, or simply, a *standard set*. Write v_i for (x_i, y_i). For any integer m, where $1 \leq m < N$, the *m-division of S*, $(D_1(S), D_2(S), D_3(S), D_4(S))$ is a partition of S into four disjoint subsets $D_i(S)$ defined as follows: $D_4(S) = A_1(S) \cap A_2(S)$, $D_2(S) = A_1(S) - D_4(S)$, $D_3(S) = A_2(S) - D_4(S)$, $D_1(S) = S - D_2(S) - D_3(S) - D_4(S)$, where $A_1(S)$ is the subset of v_i with the m largest x_i, and $A_2(S)$ is the subset of $\tilde{v}_i$ with the m largest y_i. (See Figure 1.) We also define $D_5(S) = \emptyset$ if $D_4(S) \neq \emptyset$, and otherwise let $D_5(S) = D_1(S) \cap ((c,1) \times (d,1))$, where $c = \max\{x_j \mid v_j \in D_3(S)\}$ and $d = \max\{y_i \mid v_i \in D_2(S)\}$. (See Figure 2.) For convenience, we agree that the emptyset $\emptyset$ is a standard N-set with $N = 0$, and $D_i(\emptyset) = \emptyset$ for $1 \leq i \leq 5$.

[2]A *right-to-left maximum* in $A[1:m]$ is a location $1 \leq i \leq m$ such that $A[i] > A[k]$ for all $i < k \leq m$. For example, the array $A[1\colon 7] = (2,5,9,3,7,1,4)$ has right-to-left maxima at $i = 7, 5$, and 3.

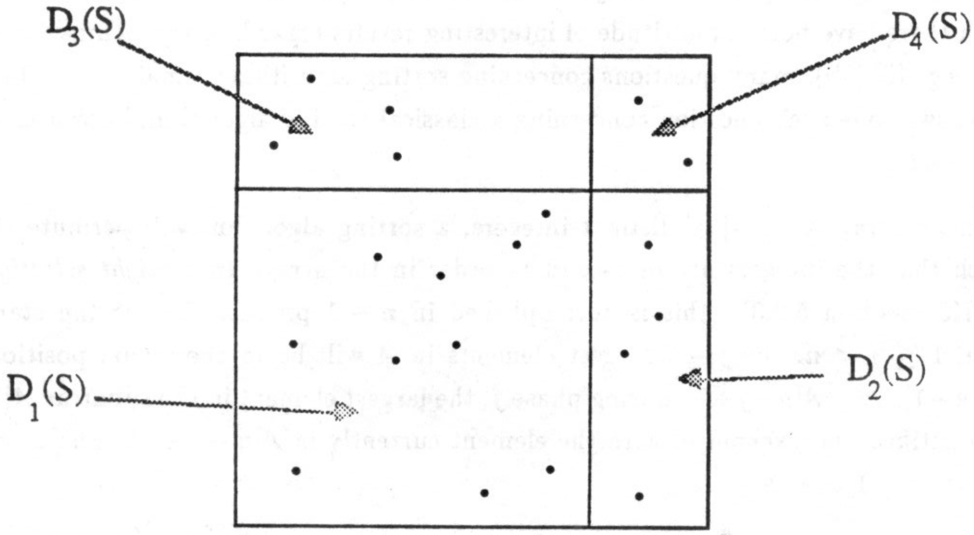

Figure 1: A 6 - division

A point (x,y) *dominates* a point (x',y') if $(x,y) \neq (x',y')$ and $x \geq x'$, $y \geq y'$. Let T be a standard set. A point $(x,y) \in T$ is a *maximal point of* T if no point in T dominates (x,y). Let $MAX(T)$ denote the set of all maximal points of T. Let $MAX(T) = \emptyset$ if $T = \emptyset$.

Take a random set S of N points $v_i = (x_i, y_i)$, when each x_i, y_j is uniformly and independently chosen from the interval $[0,1]$. Call S thus generated a *uniform random N-set.* It is clear that, with probability 1, a uniform random N-set is a standard N-set. Let $1 \leq m < N$, and $1 \leq i \leq 5$. Let $(D_1(S),\ D_2(S),\ D_3(S),\ D_4(S))$ be the m-division of S, and $D_5(S)$ be defined as before. Denote by $r_{N,m,i}$ the random variable corresponding to $|MAX(D_i(S))|$. The next two theorems give an explicit formula for $Var(B_n)$. Let $H_N^{(2)}$ denote $\sum_{1\leq j\leq N}(1/j^2)$.

Theorem 1 For all $n > 1$,

$$Var(B_n) = \sum_{1<N\leq n} (H_N - H_N^{(2)}) + 2 \sum_{1<N\leq n} \sum_{1\leq m\leq N-2} \Big(E(r_{N,m,5}\, r_{N,m,1}) - E(r_{N,m,5})\, H_{N-m} \Big) .$$

Definition 1 Let N, m, k, ℓ be integers such that $1 \leq m \leq N-2$, $k, \ell \geq 0$. Let $0 < \lambda,\ \lambda' < 1$. Define

$$p_{N,m} = \binom{N-m}{m} \Big/ \binom{N}{m} ,$$

$$h_{N,m}(\lambda, \lambda', k) = m^2 \binom{N-2m}{k} (1-\lambda)^{m-1} (1-\lambda')^{m-1} (\lambda\lambda')^k (1-\lambda\lambda')^{N-2m-k} ,$$

and, for $0 < z < 1$,

$$q_{N,m,k,\ell}(\lambda,\lambda',z) = k \binom{N-2m-k}{\ell} (1-z)^{k-1} \Big(\frac{\lambda'(1-\lambda)z}{1-\lambda\lambda'}\Big)^{\ell} \Big(1 - \frac{\lambda'(1-\lambda)z}{1-\lambda\lambda'}\Big)^{N-2m-k-\ell} .$$

Theorem 2 For all integers m, N with $1 \leq m \leq N-2$,

$$E(r_{N,m,5}) = p_{N,m} \sum_{k\geq 1} H_k \int_0^1 \int_0^1 h_{N,m}(\lambda,\lambda',k)\, d\lambda\, d\lambda' ,$$

and

$$\begin{aligned} E(r_{N,m,5}\, r_{N,m,1}) &= p_{N,m} \sum_{k\geq 1} \Big(H_k^2 + H_k - H_k^{(2)} \Big) \int_0^1 \int_0^1 h_{N,m}(\lambda,\lambda',k)\, d\lambda\, d\lambda' \\ &+ 2p_{N,m} \sum_{k\geq 1} \sum_{\ell\geq 1} H_k H_\ell \int_0^1 \int_0^1 \int_0^1 h_{N,m}(\lambda,\lambda',k)\, q_{N,m,k,\ell}(\lambda,\lambda',z) d\lambda\, d\lambda'\, dz . \end{aligned}$$

The next theorem gives the asymptotic behavior of $Var(B_n)$. Let α be the constant of $\frac{4}{3}\sqrt{\pi} - \frac{2}{3}\sqrt{\pi} \sum_{m\geq 1} \frac{4^m((m-1)!)^2}{(2m+1)!} - \frac{4}{3}\sqrt{\pi} \sum_{m\geq 1} \frac{1}{m(2m+1)^2}$. It is easy to check that $\alpha > 0$. Let $\kappa = 1/200$.

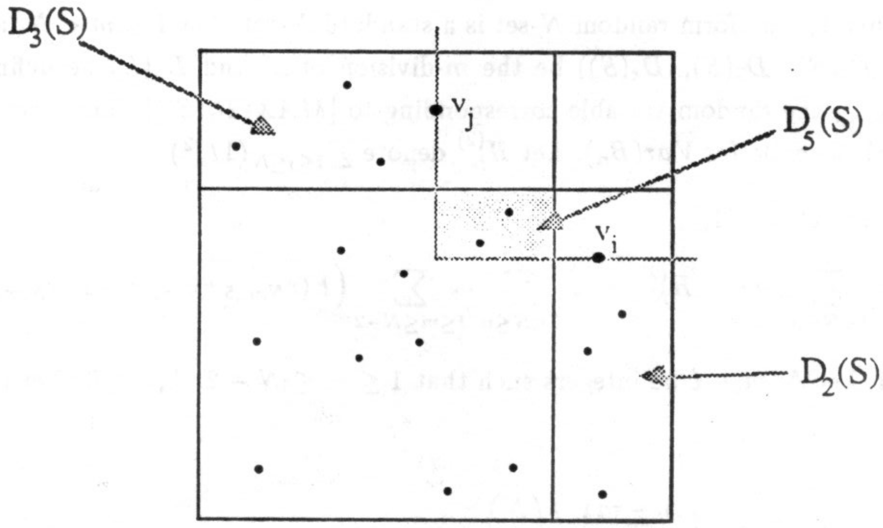

Figure 2: Illustration of $D_5(S)$

Theorem 3 For large n, $Var(B_n) = \alpha n^{3/2} + O\left(n^{3/2-\kappa} \log n\right)$.

The rest of the paper is divided into seven sections and three appendices. In Section 2 we describe a representation of the straight selection sort in terms of a two-dimensional geometric process. In Sections 3 and 4, we establish Theorem 1 and Theorem 2, respectively. In Section 5, we list a number of analytic formulas, whose proofs will be relegated to the three appendices. With the assistance of these formulas, the proof of Theorem 3 is presented in Sections 6 - 8.

How good is $\alpha n^{3/2}$ as an approximation of $Var(B_n)$? We conjecture that the error term given in Theorem 3 is far too high. We leave as an interesting open problem a better determination of the second-order term in the asymptotic expansion of $Var(B_n)$.

2 A Geometric Representation

In this section we consider a representation of the straight selection sort as a geometric process, which is the underlying basis for our approach. We will also prove several elementary properties of two-dimensional point sets that will be of use in Sections 3 and 4.

For any standard N-set T with $N \geq 1$, we define the notion of *derived set* $d(T)$. Let $(x_i, y_i), (x_j, y_j) \in T$ be, respectively, the points in T with the largest x-coordinate and the point with the largest y-coordinate. That is, $x_i = \max\{z \mid (z, z') \in T\}$ and $y_j = \max\{z' \mid (z, z') \in T\}$. Let $d(T) = (T - \{(x_i, y_i), (x_j, y_j)\}) \cup \{(x_j, y_i)\}$ if $(x_i, y_i) \neq (x_j, y_j)$, and $d(T) = T - \{(x_j, y_i)\}$ if $(x_i, y_i) = (x_j, y_j)$. Clearly, $d(T)$ is a standard $(N-1)$-set. Let us further define $d^{(0)}(T) = T$, and $d^{(m)}(T) = d(d^{(m-1)}(T))$ for $1 \leq m \leq |T| - 1$.

For $N \geq 1$, let Σ_N be the set of all permutations of $(1, 2, \ldots, N)$. For any $\rho = (\rho(1), \rho(2), \ldots, \rho(N)) \in \Sigma_N$, let $V(\rho)$ denote the standard N-set $\{(i, \rho(i)) \mid 1 \leq i \leq N\}$. Let R_ρ be the set of *right-to-left maxima* in ρ, i.e. $R_\rho = \left\{j \mid 1 \leq j \leq N,\ \rho(j) > \rho(k) \text{ for all } j < k \leq N\right\}$. We further agree that, for $N = 0$, $\Sigma_N = \{\lambda_\phi\}$, where λ_ϕ is a special symbol; define $V(\lambda_\phi) = \emptyset$.

Lemma 1 $MAX(V(\rho)) = \{(j, \rho(j)) \mid j \in R_\rho\}$.

Proof. Let $\rho \in \Sigma_N$. If $N = 0$, the lemma is obviously true. We can thus assume $N > 0$. If $(j, \rho(j)) \in MAX(V(\rho))$, then $\rho(j) > \rho(k)$ for all $j < k$. Thus, $j \in R_\rho$. In the other direction, if $j \in R_\rho$, then there cannot exist $(k, \rho(k))$ with $k > j$ and $\rho(k) > \rho(j)$. This implies $(j, \rho(j)) \in MAX(V(\rho))$. □

Let $N > m \geq 0$. For any $\rho \in \Sigma_N$, let $\rho^{(m)}$ denote the subarray $A[1 : N - m]$ at the start of the $(m+1)$-st phase of the straight selection sort, assuming that $A[1 : N]$ is initially set by $A[i] \leftarrow \rho(i)$ for $1 \leq i \leq N$. We will also regard $\rho^{(m)}$ as an element in Σ_{N-m+1} in the obvious way.

Lemma 2 $V(\rho^{(m)}) = d^{(m)}(V(\rho))$.

Proof. We prove it by induction on $m \geq 0$. The induction base $m = 0$ is clearly true. Inductively, let $N > m > 0$, and assume that we have already proved $V(\rho^{(m-1)}) = d^{(m-1)}(V(\rho))$. Let j_0 be such that $\rho^{(m-1)}(j_0) = N - m + 1$. There are two cases. If $j_0 \neq N - m + 1$, then $\rho^{(m)}(j) = \rho^{(m-1)}(j)$ for $j \in \{1, 2, \ldots, N - m\} - \{j_0\}$ and $\rho^{(m)}(j_0) = \rho^{(m-1)}(N - m + 1)$; thus $V(\rho^{(m)})$ will be $\left(V(\rho^{(m)}) - \left\{\left(N - m + 1,\ \rho^{(m-1)}(N - m + 1)\right),\ \left(j_0, \rho^{(m-1)}(j_0)\right)\right\}\right) \cup \{(j_0, \rho^{(m-1)}(N - m + 1))\} = d(V(\rho^{(m-1)})$, which by the induction hypothesis, equals $d\left(d^{(m-1)}(V(\rho))\right) = d^{(m)}(V(\rho))$. In the other case, $j_0 = N - m + 1$, and $\rho^{(m)}(j) = \rho^{(m-1)}(j)$ for all $j \in \{1, 2, \ldots, N - m\}$; by the induction hypothesis $V(\rho^{(m-1)}) = d^{(m-1)}(V(\rho))$, we have then $V(\rho^{(m)}) = V(\rho^{(m-1)}) - \{(N - m + 1, N - m + 1)\} = d\left(V(\rho^{(m-1)})\right) = d\left(d^{(m-1)}((\rho))\right) = d^{(m)}(V(\rho))$. This completes the inductive step. □

Remark. We can thus view the straight selection sort of $\rho \in \Sigma_n$ as the transformation of a standard set $V(\rho) \to d^{(1)}(V(\rho)) \to d^{(2)}(V(\rho)) \to \ldots \to d^{(n-1)}(V(\rho))$, with $\left|MAX\left(d^{(m-1)}(V(\rho))\right)\right| - 1$ as the cost $C_{n,m} - 1$ for the m-th phase, where $1 \leq m < n$. This connection is the underlying basis of our approach to the analysis of straight selection sort, as it links the sorting problem to a geometric process in two dimensions.

Definition 2 Let T be any finite set of points in the plane. The *dual* of T is defined as $dual(T) = \{(y,x) \mid (x,y) \in T\}$.

Lemma 3 If $\rho \in \Sigma_N$, then $V(\rho^{-1}) = \text{dual}\ (V(\rho))$.

Proof. If $N = 0$, then $V(\rho^{-1}) = \emptyset = \text{dual}(V(\rho))$. If $N > 0$, then $\text{dual}(V(\rho)) = \left\{(\rho(i), i) \mid 1 \leq i \leq N\right\} = \left\{(j, \rho^{-1}(j)) \mid 1 \leq j \leq N\right\} = V(\rho^{-1})$. □

Lemma 4 For any two finite sets T, T' of points in the plane, we have

$$\text{dual}(T \cup T') = \text{dual}(T) \cup \text{dual}(T') \ ,$$

and

$$\text{dual}(T \cap T') = \text{dual}(T) \cap \text{dual}(T') \ .$$

Proof. Immediate from the definitions. □

Lemma 5 For any standard set T, we have

$$\begin{aligned} MAX(\text{dual}(T)) &= \text{dual}(MAX(T)) \ , \\ D_2(\text{dual}(T)) &= \text{dual}(D_3(T)) \ , \\ D_3(\text{dual}(T)) &= \text{dual}(D_2(T)) \ , \\ D_i(\text{dual}(T)) &= \text{dual}(D_i(T)) \ \textit{for} \ i \in \{1,4,5\}. \end{aligned}$$

Proof. Immediate from the definitions. □

Lemma 6 Let $N > m \geq 0$. For any standard N-set T, we have $d^{(m)}(\text{dual}(T)) = \text{dual}(d^{(m)}(T))$.

Proof. A straightforward proof by induction on m. □

3 Proof of Theorem 1

3.1 Reduction

By definition, $B_n = \sum_{1\le j<n}(C_{n,j}-1)$, and thus,

$$\begin{aligned} Var(B_n) &= E\Big(B_n^2\Big) - \Big(E(B_n)\Big)^2 \\ &= E\bigg(\Big(\sum_{1\le j<n} C_{n,j}\Big)^2\bigg) - \bigg(\sum_{1\le j<n} E\Big(C_{n,j}\Big)\bigg)^2 \\ &= \sum_{1\le j<n} E(C_{n,j}^2) + 2\sum_{1\le j<n}\sum_{j<\ell<n} E(C_{n,j}\,C_{n,\ell}) \\ &\qquad - \sum_{1\le j<n}(E(C_{n,j}))^2 - 2\sum_{1\le j<n}\sum_{j<\ell<n} E(C_{n,j})\,E(C_{n,\ell}) \\ &= \sum_{1\le j<n} Var(C_{n,j}) + 2\sum_{1\le j<n}\sum_{j<\ell<n}\Big\{E(C_{n,j}\,C_{n,\ell}) - E(C_{n,j})\,E(C_{n,\ell})\Big\}\ . \qquad (1) \end{aligned}$$

It is well known (see [K3, Section 5.2.3]) that, if we start with a random array A, then at the start of phase j, the array $A[1:n-j+1]$ is random, in the sense that all $(n-j+1)!$ relative orderings of the $n-j+1$ integers in it are equally likely. This implies (see [K2, Section 1.2.10 Eq. (16)]) that, for $1\le j<n$,

$$E(C_{n,j}) = H_{n-j+1}\ , \qquad (2)$$

and

$$Var(C_{n,j}) = H_{n-j+1} - H_{n-j+1}^{(2)}\ . \qquad (3)$$

It also implies that, for all $1\le j<\ell<n$,

$$E(C_{n,j}\,C_{n,\ell}) = E(C_{n-j+1,1}\,C_{n-j+1,\ell-j+1})\ , \qquad (4)$$

$$E(C_{n,j}) = E(C_{n-j+1,1})\ , \qquad (5)$$

and

$$E(C_{n,\ell}) = E(C_{n-\ell+1,1})\ . \qquad (6)$$

From (1) - (6), we obtain, for $n\ge 2$,

$$\begin{aligned} Var(B_n) &= \sum_{1<N\le n}\Big(H_N - H_N^{(2)}\Big) \\ &\quad + 2\sum_{1<N\le n}\sum_{1\le m\le N-2}\Big\{E(C_{N,1}\,C_{N,m+1}) - E(C_{N,1})\,E(C_{N,m+1})\Big\}\ . \qquad (7) \end{aligned}$$

We will prove that, for all $1 \leq m \leq N-2$,

$$E(C_{N,1}\, C_{N,m+1}) - E(C_{N,1})\, E(C_{N,m+1}) = E(r_{N,m,5}\, r_{N,m,1}) - E(r_{N,m,5})\, E(C_{N,m+1}) \ . \tag{8}$$

Clearly, Theorem 1 follows from (7), (8), and (2). The rest of this section is devoted to a proof of Equation (8). We will assume m, N to be fixed, with $1 \leq m \leq N-2$, for the remainder of Section 3.

3.2 Notations and Simple Facts

Definition 3 Let $\rho = (\rho(1), \rho(2), \ldots, \rho(N)) \in \Sigma_N$. We partition $\{1, 2, \ldots, N\}$ into disjoint parts $I_i(\rho)$, $1 \leq i \leq 4$, as follows:

$$\begin{cases} I_1(\rho) = \{j | 1 \leq j \leq N-m, & \rho(j) \leq N-m\}\ , \\ I_2(\rho) = \{j | N-m < j \leq N, & \rho(j) \leq N-m\}\ , \\ I_3(\rho) = \{j | 1 \leq j \leq N-m, & \rho(j) > N-m\}\ , \\ I_4(\rho) = \{j | N-m < j \leq N, & \rho(j) > N-m\}\ . \end{cases}$$

Let $\rho^{<i>}$ be the subarray of ρ restricted to positions in $I_i(\rho)$.

Remark. We shall use the special symbol μ_ϕ to stand for the unique sequence of length 0. In the above definition, if $I_i(\rho) = \emptyset$, then $\rho^{<i>} = \mu_\phi$.

Clearly, if $\ell = |I_4(\rho)|$, then $0 \leq \ell \leq m$, $|I_2(\rho)| = |I_3(\rho)| = m - \ell$, and $|I_1(\rho)| = N - 2m + \ell$.

Definition 4 For $0 \leq \ell \leq m$, let $\Sigma_{N,m,\ell} = \{\rho \mid \rho \in \Sigma_N\ ,\ |I_4(\rho)| = \ell\}$.

Definition 5 For any $\rho \in \Sigma_N$ and $1 \leq i \leq 4$, let $R_{\rho,i} = R_\rho \cap I_i(\rho)$.

Example 1 Let $N = 9$, $m = 4$, and $\rho = (3,9,5,6,7,8,4,1,2)$, then $\rho \in \Sigma_{9,4,1}$, $I_1(\rho) = \{1,3\}$, $I_2(\rho) = \{7,8,9\}$, $I_3(\rho) = \{2,4,5\}$, and $I_4(\rho) = \{6\}$. Also, $\rho^{<1>} = (3,5)$, $\rho^{<2>} = (4,1,2)$, $\rho^{<3>} = (9,6,7)$, $\rho^{<4>} = (8)$, and $R_\rho = \{9,7,6,2\}$.

Lemma 7 If $\rho \in \Sigma_N$, then $D_i(V(\rho)) = \left\{(j, \rho(j)) \mid j \in I_i(\rho)\right\}$ for $1 \leq i \leq 4$.

Proof. Immediate from the definitions. □

Lemma 8 If $\rho \in \Sigma_N$, then, for $1 \leq i \leq 4$,

$$D_i(V(\rho)) \cap\ MAX(V(\rho)) = \left\{(j, \rho(j)) \mid j \in R_{\rho,i}\right\}\ .$$

Proof. Immediate from the definitions and Lemmas 1, 7. □

Example 2 In Figure 3 we show the set $V(\rho)$ where ρ is as in Example 1. Note that $D_3(V(\rho)) = \{(2,9),(4,6),(5,7)\}$, and $MAX(V(\rho)) = \{(2,9),(6,8),(7,4),(9,2)\}$. This agrees with the statements in Lemmas 1, 7 and 8.

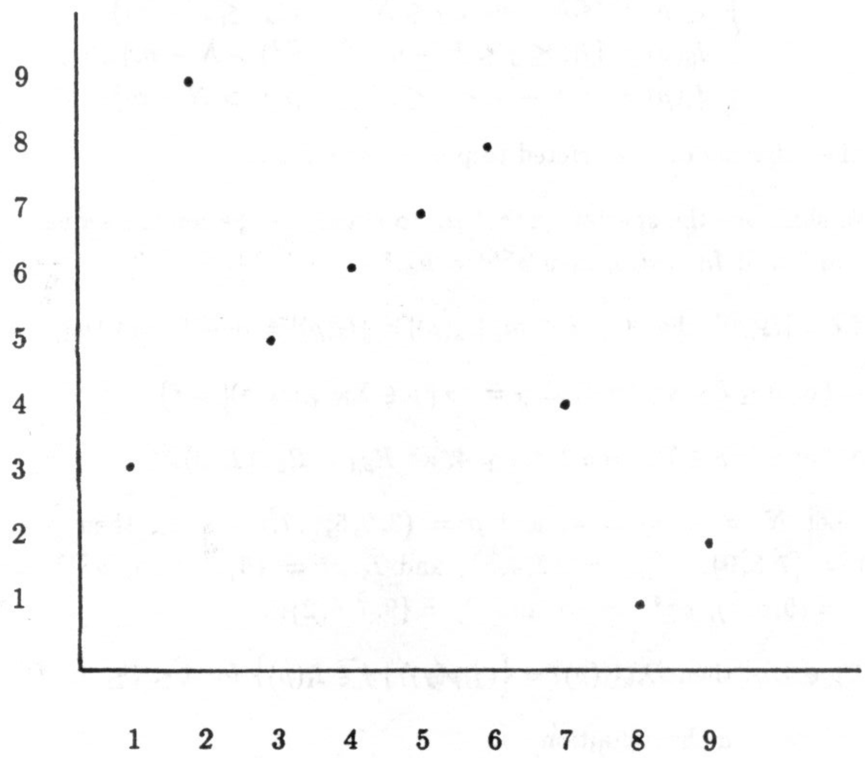

Figure 3: $V(\rho)$ for $\rho = (3,9,5,6,7,8,4,1,2)$; $N = 9$, $m = 4$.

Lemma 9 If $\rho \in \Sigma_N$, then $|R_{\rho^{-1},2}| = |R_{\rho,3}|$ and $|R_{\rho^{-1},3}| = |R_{\rho,2}|$.

Proof. From Lemma 8 and Lemma 3,

$$\begin{aligned} |R_{\rho^{-1},2}| &= |D_2(V(\rho^{-1})) \cap MAX(V(\rho^{-1}))| \\ &= \left|D_2\Big(\mathrm{dual}(V(\rho))\Big) \cap MAX\Big(\mathrm{dual}(V(\rho))\Big)\right| . \end{aligned} \tag{9}$$

By Lemma 5,

$$D_2\Big(\mathrm{dual}(V(\rho))\Big) = \mathrm{dual}\Big(D_3(V(\rho))\Big) , \tag{10}$$

and

$$MAX\Big(\mathrm{dual}(V(\rho))\Big) = \mathrm{dual}\Big(MAX(V(\rho))\Big) . \tag{11}$$

It follows from (9), (10), (11), and Lemma 4 that

$$\begin{aligned} |R_{\rho^{-1},2}| &= \left|\mathrm{dual}\Big(D_3(V(\rho)) \cap MAX(V(\rho))\Big)\right| \\ &= \left|D_3(V(\rho)) \cap MAX(V(\rho))\right| . \end{aligned}$$

Hence, from Lemma 8, we have

$$|R_{\rho^{-1},2}| = |R_{\rho,3}| .$$

This proves one of the equalities in the lemma. The other equality $|R_{\rho^{-1},3}| = |R_{\rho,2}|$ can be established similarly. □

3.3 First Step

Take a random ρ, uniformly chosen from Σ_N, and let R_i , $1 \leq i \leq 4$ denote the random variable corresponding to $|R_{\rho,i}|$. In this subsection, we will prove that

$$\begin{aligned} E(C_{N,1}\, C_{N,m+1}) &- E(C_{N,1})E(C_{N,m+1}) \\ &= E(R_1\, C_{N,m+1}) - E(R_1)E(C_{N,m+1}) . \end{aligned} \tag{12}$$

To this end, it is clearly sufficient to prove that, for each $i \in \{2, 3, 4\}$,

$$E(R_i\, C_{N,m+1}) = E(R_i)E(C_{N,m+1}) , \tag{13}$$

as $C_{N,1} = \sum_{1 \leq j \leq 4} R_j$.

We begin by devising a method of generating a random ρ, which will enable us to examine $E(R_i\, C_{N,m+1})$ conveniently in detail.

Definition 6 Let $s > 0$ be an integer. For any s-tuple of distinct real numbers $x = (x_1, x_2, \ldots, x_s)$, let $\tau(x)$ denote the permutation $(i_1, i_2, \ldots, i_s) \in \Sigma_s$ such that x_j is the i_j-th smallest element among $(x_1, x_2, \ldots, x_s)$.

Remark. We agree that $\tau(\mu_\phi) = \lambda_\phi$. Recall that $\Sigma_s = \{\lambda_\phi\}$ for $s = 0$ in our convention.

Definition 7 Let $s, t \geq 0$ be integers, not both zero. Denote by $\Gamma_{s,t}$ the family of all subsets $W \subseteq \{1, 2, \ldots, s+t\}$ with $|W| = s$. Let $x = (x_1, x_2, \ldots, x_s)$ and $y = (y_1, y_2, \ldots, y_t)$ be tuples of real numbers, where $x_1, x_2, \ldots, x_s$, $y_1, y_2, \ldots, y_t$ are all distinct. Define $\tau(x, y)$ as the subset $W \in \Gamma_{s,t}$ such that, for each $i \in W$, the i-th smallest element among $x_1, x_2, \ldots, x_s$, $y_1, y_2, \ldots, y_t$ is in $\{x_1, x_2, \ldots, x_s\}$.

Informally, $\tau(x)$ specifies the relative ordering among the componenets of x, and $\tau(x, y)$ specifies the the merge pattern between x and y. For example, if $x = (2.8, 4.3, 1.1, 25)$, $y = (16, 1.4, 5.2)$, then $\tau(x) = (2, 3, 1, 4)$ and $\tau(x, y) = \{1, 3, 4, 7\}$.

Definition 8 Let ℓ be any integer satisfying $0 \leq \ell \leq m$. Let

$$\begin{aligned}\Delta_{N,m,\ell} = \Gamma_{N-2m+\ell, m-\ell} \;&\times\; \Gamma_{m-\ell,\ell} \times \Gamma_{N-2m+\ell, m-\ell} \times \Gamma_{m-\ell,\ell} \\ &\times\; \Sigma_{N-2m+\ell} \times \Sigma_{m-\ell} \times \Sigma_{m-\ell} \times \Sigma_\ell \;.\end{aligned}$$

Lemma 10 For each $\delta \in (\xi_{13}, \xi_{24}, \eta_{12}, \eta_{34}, \sigma_1, \sigma_2, \sigma_3, \sigma_4) \in \Delta_{N,m,\ell}$, there exists a unique $\rho \in \Sigma_{N,m,\ell}$ such that the following conditions are satisfied: $\tau(I_1(\rho), I_3(\rho)) = \xi_{13}$, $\tau(I_2(\rho), I_4(\rho)) = \xi_{24}$, $\tau(\rho^{<1>}, \rho^{<2>}) = \eta_{12}$, $\tau(\rho^{<3>}, \rho^{<4>}) = \eta_{34}$, and $\tau(\rho^{<i>}) = \sigma_i$ for $1 \leq i \leq 4$.

Proof. Let $J_1 = \xi_{13}$, $J_2 = \{N - m + j \mid j \in \xi_{24}\}$, $J_3 = \{1, 2, \ldots, N-m\} - J_1$, $J_4 = \{N - m + j \mid 1 \leq j \leq m\} - J_2$, $K_1 = \eta_{12}$, $K_2 = \{1, 2, \ldots, N-m\} - K_1$, $K_3 = \{N - m + j \mid j \in \eta_{34}\}$, and $K_4 = \{N - m + j \mid 1 \leq j \leq m\} - K_3$. Clearly, J_1, J_2, J_3, J_4 form a partition of $\{1, 2, \ldots, N\}$; so do K_1, K_2, K_3, K_4.

For each $1 \leq i \leq 4$ with $J_i \neq \emptyset$, let $\varphi_i : J_i \rightarrow K_i$ be the unique $1-1$ mapping such that, if $J_i = \{j_1, j_2, \ldots, j_t\}$ with $j_1 < j_2 < \ldots < j_t$, then $\tau((\varphi_i(j_1), \varphi_i(j_2), \ldots, \varphi_i(j_t))) = \sigma_i$. Let $\rho \in \Sigma_N$ be defined by $\rho(j) = \varphi_i(j)$ if $j \in J_i$. It is straightforward to verify that $\rho \in \Sigma_{N,m,\ell}$ and all the specifications for ρ stated in the lemma are met.

To show the uniqueness, assume $\rho' \in \Sigma_{N,m,\ell}$ also satisfies all the specifications. Clearly, the constraints imposed by $\xi_{13}, \xi_{24}, \eta_{12}, \eta_{34}$ imply that $I_i(\rho) = I_i(\rho')$, and $\{\rho(j) \mid j \in I_i(\rho)\} = \{\rho'(j) \mid j \in I_i(\rho')\}$ for $1 \leq i \leq 4$. Then, for each $1 \leq i \leq 4$, the constraint $\tau(\rho^{<i>}) = \tau(\rho'^{<i>})$ implies that $\rho(j) = \rho'(j)$ for $j \in I_i(\rho)$. This proves $\rho = \rho'$. □

Definition 9 For each $\delta \in \Delta_{N,m,\ell}$, let χ_δ denote the $\rho \in \Sigma_{N,m,\ell}$ associated with δ in Lemma 10.

Clearly, for any $\rho \in \Sigma_{N,m,\ell}$, there exists a $\delta \in \Delta_{N,m,\ell}$, such that $\chi_\delta = \rho$. Thus, $\rho = \chi_\delta$ gives a $1-1$ correspondence between $\Sigma_{N,m,\ell}$ and $\Delta_{N,m,\ell}$.

Example 3 Consider the permutation ρ given in Examples 1 and 2, with $N = 9$, $m = 4$, and $\rho = (3, 9, 5, 6, 7, 8, 4, 1, 2)$. Let $\delta = (\xi_{13}, \xi_{24}, \eta_{12}, \eta_{34}, \sigma_1, \sigma_2, \sigma_3, \sigma_4) \in \Delta_{N,m,\ell}$, where $\ell = 1, \xi_{13} = \{1, 3\}$,

$\xi_{24} = \{2,3,4\}$, $\eta_{12} = \{3,5\}$, $\eta_{34} = \{1,2,4\}$, $\sigma_1 = (1,2)$, $\sigma_2 = (3,1,2)$, $\sigma_3 = (3,1,2)$, and $\sigma_4 = (1)$. It can be readily verified that $\rho = \chi_\delta$ as specified in Lemma 10.

Lemma 11 Generate a random $\delta = (\xi_{13}, \xi_{24}, \eta_{12}, \eta_{34}, \sigma_1, \sigma_2, \sigma_3, \sigma_4) \in \Delta_{N,m,\ell}$, where each component is uniformly and independently chosen from its domain, and let $\rho = \chi_\delta$. Then ρ is uniformly distributed over $\Sigma_{N,m,\ell}$.

Proof. It follows immediately from Lemma 10 and the remark after Definition 9. □

We now describe our approach to the proof of (13). Let us concentrate on the case $i = 2$. To evaluate $E(R_2 C_{N,m+1})$, we first generate a random $0 \leq \ell \leq m$ according to some appropriate probability distribution, and then randomly choose a $\delta \in \Delta_{N,m,\ell}$; the expected value of the random variable $|R_{\rho,2}| \cdot |R_{\rho^{(m)}}|$, where $\rho = \chi_\delta$, is then equal to $E(R_2 C_{N,m+1})$. Let $\delta = (\xi_{13}, \xi_{24}, \eta_{12}, \eta_{34}, \sigma_1, \sigma_2, \sigma_3, \sigma_4)$. It will be seen that the value of $|R_{\rho,2}|$ is determined by $\xi_{24}, \sigma_2, \sigma_4$. We can thus evaluate the expected value of $|R_{\rho,2}| \cdot |R_{\rho^{(m)}}|$, by first fixing the values of $\xi_{24}, \sigma_2, \sigma_4$ and calculate the conditional expected value of $|R_{\rho^{(m)}}|$. It turns out that, for any fixed $\xi_{24}, \sigma_2, \sigma_4$, if we randomize over the remaining components of δ, we obtain a $\rho = \chi_\delta$ with $\rho^{(m)}$ distributed as a uniform random element from Σ_{N-m}. This implies that, for any fixed $\xi_{24}, \sigma_2, \sigma_4$, the conditional expected value of $|R_{\rho^{(m)}}|$ is equal to $E(C_{N-m+1})$. We can thus effectively replace the random variable $|R_{\rho^{(m)}}|$ by the constant $E(C_{N-m+1})$ in the expression $|R_{\rho,2}| \cdot |R_{\rho^{(m)}}|$, whose expected value was to be calculated. Taking out the constant factor $E(C_{N-m+1})$, we obtain the final expected value $E(R_2) \cdot E(C_{N-m+1})$.

Below, Lemma 12 shows that $|R_{\rho,2}|$ is determined by $\xi_{24}, \sigma_2, \sigma_4$. Lemma 13 expresses $\rho^{(m)}$ in terms of the other components of δ, and in Lemma 14 $\rho^{(m)}$ is shown to be uniformly distributed over Σ_{N-m}, when these components are randomized.

Remark. The statements and proofs of Lemmas 12, 13, and 14 are presented without reference to the two-dimensional representation of permutations ρ as given in Section 2. However, it may be helpful to understand the proofs, if we keep in mind the interpretation of ρ as $V(\rho)$, $\rho^{(m)}$ as $d^{(m)}(V(\rho))$, and the components of δ as various ordering relations either between the sets $D_i(V(\rho))$ or among the points in one of these sets. For example, ξ_{13} specifies how the x-coordinates of the points in $D_1(V(\rho))$ interleave with those of the points in $D_3(V(\rho))$; η_{12} specifies how the y-coordinates of the points in $D_1(V(\rho))$ interleave with those of the points in $D_2(V(\rho))$; σ_1 specifies the relative ordering of points in $D_1(V(\rho))$ as a two-dimensional set.

Lemma 12 There exist real-valued functions v, w on $\Gamma_{m-\ell,\ell} \times \Sigma_{m-\ell} \times \Sigma_\ell$ such that $|R_{\chi_\delta,2}| = v(\xi_{24}, \sigma_2, \sigma_4)$ and $|R_{\chi_\delta,4}| = w(\xi_{24}, \sigma_2, \sigma_4)$, if $\delta = (\xi_{13}, \xi_{24}, \eta_{12}, \eta_{34}, \sigma_1, \sigma_2, \sigma_3, \sigma_4) \in \Delta_{N,m,\ell}$.

Proof. Straightforward from the definitions. □

Definition 10 Let $\xi_{13}, \eta_{12} \in \Gamma_{N-2m+\ell,m-\ell}$, $\sigma_1 \in \Sigma_{N-2m+\ell}$, and $\zeta \in \Sigma_{m-\ell}$. Write $J_3 = \{1,2,\ldots,N-m\} - \xi_{13}$ and $K_2 = \{1,2,\ldots,N-m\} - \eta_{12}$. Suppose $\xi_{13} = \{i_1, i_2, \ldots, i_{N-2m+\ell}\}$,

$\eta_{12} = \{i'_1, i'_2, \ldots, i'_{N-2m+\ell}\}$, $J_3 = \{j_1, j_2, \ldots j_{m-\ell}\}$ and $K_2 = \{k_1, k_2, \ldots, k_{m-\ell}\}$, where the elements of each set are listed in ascending order. Define $b(\xi_{13}, \eta_{12}, \sigma_1, \zeta)$ to be the $(N-m)$-tuple $c = (c_1, c_2, \ldots, c_{N-m}) \in \Sigma_{N-m}$, where $c_{i_r} = i'_{\sigma_1(r)}$ for $1 \le r \le N-2m+\ell$, and $c_{j_s} = k_{\zeta(s)}$ for $1 \le s \le m-\ell$.

Remark. In other words, if we have array $A[1:N-m]$ with $A[i_r] = i'_{\sigma_1(r)}$ for $1 \le r \le N-2m+\ell$, and $A[j_s] = +\infty$ for $1 \le s \le m-\ell$, then we can obtain c by replacing the ∞ entries with items in K_2, and in fact, $A[j_s]$ gets the $\zeta(s)$-th smallest element of K_2.

Let $k > 0$. For any two elements $\beta, \beta' \in \Sigma_k$, their *product* $\beta\beta'$ is defined as usual to be the element $\gamma \in \Sigma_k$ with $\gamma(i) = \beta(\beta'(i))$ for all $1 \le i \le k$. We agree that, for $k = 0$, the product $\lambda_\phi \lambda_\phi$ is λ_ϕ.

Lemma 13 There exists a mapping $u : \Gamma_{m-\ell,\ell} \times \Gamma_{m-\ell,\ell} \times \Sigma_{m-\ell} \times \Sigma_\ell \to \Gamma_{m-\ell}$ such that the following is true: for any $\rho = \chi_\delta$, where $\delta = (\xi_{13}, \xi_{24}, \eta_{12}, \eta_{34}, \sigma_1, \sigma_2, \sigma_3, \sigma_4) \in \Delta_{N,m,\ell}$, we have $\rho^{(m)} = b(\xi_{13}, \eta_{12}, \sigma_1, \zeta\sigma_3)$ where $\zeta = u(\xi_{24}, \eta_{34}, \sigma_2, \sigma_4)$.

Remark. The detailed proof to be given below is long. We explain here why it is plausible. Consider an array $A[1:N]$, with $A[i] = \rho(i)$ initially. After m phases of the straight selection sort having been applied to A, the subarray $A[1:N-m]$ now contains $\rho^{(m)}$. Since no locations $i \in I_1(\rho)$ in array A were involved in the first m phases, $\rho^{(m)}$ can be obtained directly from the original subarray $A[1:N-m]$, by replacing items in $A[i]$, $i \in I_3(\rho)$, with items in $\{\rho(j) \mid j \in I_2(\rho)\}$. It is thus clear (see the remark after Definition 10) that $\rho^{(m)} = b(\xi_{13}, \eta_{12}, \sigma_1, \zeta')$ for some $\zeta' \in \Sigma_{m-\ell}$. It is plausible that ζ' depends only on $\xi_{24}, \eta_{34}, \sigma_2, \sigma_4$, and σ_3, since the locations $i \in I_1(\rho)$ in A do not affect the relative ordering of the items in other locations in the sorting process.

Proof of Lemma 13. If $\ell = m$, let u denote the constant mapping with value λ_ϕ. In this case $\xi_{13} = \eta_{12} = \{1, 2, \cdots, N-m\}$, $\sigma_3 = \lambda_\phi$. Therefore, $b(\xi_{13}, \eta_{12}, \sigma_1, \zeta\sigma_3) = \sigma_1$. Now, for any $\rho = \chi_\delta$, where $\delta = (\xi_{13}, \xi_{24}, \eta_{12}, \eta_{34}, \sigma_1, \sigma_2, \sigma_3, \sigma_4) \in \Delta_{N,m,\ell}$, the sorting process clearly gives $\rho^{(m)}(i) = \rho(i)$ for $1 \le i \le N-m$. It follows that $\rho^{(m)} = b(\xi_{13}, \eta_{12}, \sigma_1, \zeta\sigma_3)$ where $\zeta = u(\xi_{24}, \eta_{34}, \sigma_2, \sigma_4)$ as required by the lemma.

We can thus assume that $\ell < m$. Define $\delta' = (\xi_{13}, \xi_{24}, \eta_{12}, \eta_{34}, \sigma_1, \sigma_2, \sigma_3^{(0)}, \sigma_4) \in \Delta_{N,m,\ell}$, where $\sigma_3^{(0)} \in \Delta_{N,m,\ell}$ is the identity permutation, and let $\rho' = \chi_{\delta'}$.

Fact 1 There exists a unique $\zeta \in \Sigma_{m-\ell}$ such that $\rho'^{(m)} = b(\xi_{13}, \eta_{12}, \sigma_1, \zeta)$. Furthermore, ζ depends only on $\xi_{24}, \eta_{34}, \sigma_2, \sigma_4$.

Before proving Fact 1, let us establish some notations. Let $J_2(\rho') = \{\rho'(i) \mid i \in I_2(\rho')\}$. Then $I_3(\rho') = \{1, 2, \ldots, N-m\} - \xi_{13}$, and $J_2(\rho') = \{1, 2, \ldots, N-m\} - \eta_{12}$. Write $I_3(\rho') = \{j_1, j_2, \ldots, j_{m-\ell}\}$ and $J_2(\rho') = \{k_1, k_2, \ldots, k_{m-\ell}\}$, where the elements of each set are listed in ascending order.

We now prove Fact 1. Consider the straight selection sort applied to an array $A[1:N]$, with $A[i] = \rho'(i)$ initially. Since the locations $A[i]$ for $i \in I_1(\rho')$ contain initially only integers no greater than $N - m$, the first m phases of the sort do not affect the contents in these locations. That means $\rho'^{(m)}(i) = \rho'(i)$ for $i \in I_1(\rho)$. We have then also $\{\rho'^{(m)}(i) \mid i \in I_3(\rho')\} = \{1, 2, \ldots, N - m\} - \{\rho'^{(m)}(i) \mid i \in I_1(\rho')\} = \{1, 2, \ldots, N - m\} - \{\rho'(i) \mid i \in I_1(\rho')\} = J_2(\rho')$. Therefore, there exists a unique $\zeta \in \Sigma_{m-\ell}$ such that $\rho'^{(m)}(j_s) = k_{\zeta(s)}$ for $1 \le s \le m - \ell$. It is clear that ζ does not depend on $\xi_{13}, \eta_{12}, \sigma_1$; in fact, if we observe the sorting process in the m phases, paying attention only to the relative ordering among contents in the array A restricted to locations in $\{1, 2, \cdots, N - m\} - I_1(\rho')$, then the process looks the same for all $\xi_{13}, \eta_{12}, \sigma_1$. Therefore, ζ is determined by $\xi_{24}, \eta_{34}, \sigma_2, \sigma_4$. It is easy to verify that ζ satisfies

$$\rho'^{(m)} = b\Big(\xi_{13}, \eta_{12}, \sigma_1, \zeta\Big) \ . \tag{14}$$

This proves Fact 1.

We define a mapping $u : \Gamma_{m-\ell,\ell} \times \Gamma_{m-\ell,\ell} \times \Sigma_{m-\ell} \times \Sigma_\ell \rightarrow \Gamma_{m-\ell}$ by assigning the ζ in Fact 1 as the value of $u(\xi_{24}, \eta_{34}, \sigma_2, \sigma_4)$.

To utilize Fact 1, we need to relate $\rho^{(m)}$ to $\rho'^{(m)}$. First we prove a relation between ρ and ρ'.

Fact 2

$$I_a(\rho) \ = \ I'_a(\rho) \quad \text{for} \quad a \in \{1, 2, 3, 4\} \ , \tag{15}$$

and,

$$\rho(i) \ = \ \rho'(i) \quad \text{for} \quad i \in I_1(\rho) \cup I_2(\rho) \cup I_4(\rho) \ , \tag{16}$$

$$\rho(j_s) \ = \ \rho'\Big(j_{\sigma_3(s)}\Big) \quad \text{for} \quad 1 \le s \le m - \ell \ . \tag{17}$$

To prove Fact 2, observe that by Lemma 10, $\tau(I_2(\rho), I_4(\rho)) = \xi_{24} = \tau(I_2(\rho'), I_4(\rho'))$. This implies $I_2(\rho) = \{N - m + i \mid i \in \xi_{24}\} = I_2(\rho')$, and thus also $I_4(\rho) = I_4(\rho')$. Similarly, one can prove $I_i(\rho) = I_i(\rho')$ for $i \in \{1, 3\}$. This proves (15).

Using a similar line of argument, one can prove $\{\rho(i) \mid i \in I_a(\rho)\} = \{\rho'(i) \mid i \in I_a(\rho')\}$ for $a \in \{1, 2, 3, 4\}$, utilizing the fact that ρ and ρ' have the same η_{12}, η_{34}. However, we have by Lemma 10, $\tau(\rho^{\langle i \rangle}) = \sigma_i = \tau(\rho'^{\langle i \rangle})$ for $i \in \{1, 2, 4\}$, $\tau(\rho^{\langle 3 \rangle}) = \sigma_3$, and $\tau(\rho'^{\langle 3 \rangle}) = \sigma_3^{(0)}$. This means that $\rho(i) = \rho'(i)$ for $i \in I_1(\rho) \cup I_2(\rho) \cup I_4(\rho)$, and $\rho(j_s) = k_{\sigma_3(s)}$, $\rho'(j_s) = k_s$ for $1 \le s \le m - \ell$. This proves (16) and (17). We have proved Fact 2.

Note that (15) implies $I_3(\rho) = I_3(\rho') = \{j_1, j_2, \cdots, j_{m-\ell}\}$. Thus, (16) and (17) determine $\rho(i)$ from ρ' for every $1 \le i \le N$.

Fact 3 For $0 \le t \le m$, we have

$$\rho^{(t)}(i) = \rho'^{(t)}(i) \quad \text{for} \quad i \in \Big(I_1(\rho) \cup I_2(\rho) \cup I_4(\rho)\Big) \cap [1, N-t] \ , \tag{18}$$

$$\rho^{(t)}(j_s) = \rho'^{(t)}\Big(j_{\sigma_3(s)}\Big) \quad \text{for} \quad 1 \le s \le m - \ell \ . \tag{19}$$

This can be proved by induction on $t \ge 0$. If $t = 0$, then (18), (19) follow from (16), (17). For the inductive step, let $0 < t \le m$, and suppose that we have proved (18), (19) for $t-1$. We will prove them for t.

Suppose that $\rho'^{(t-1)}(i_0) = N - t + 1$. Then by the definition of the straight selection sort, $\rho'^{(t)}(i_0) = \rho'^{(t-1)}(N-t+1)$ if $i_0 \ne N-t+1$, and $\rho'^{(t)}(i) = \rho'^{(t-1)}(i)$ for $i \in \{1, 2, \ldots, N-t\} - \{i_0\}$. We distinguish three cases:

CASE 1: $i_0 = N-t+1$. Since $i_0 \in I_2(\rho) \cup I_4(\rho)$, we have by induction hypothesis, $\rho^{(t-1)}(i_0) = \rho'^{(t-1)}(i_0) = N - t + 1$. Thus, the sorting process leads to $\rho^{(t)}(i) = \rho^{(t-1)}(i)$ for all $1 \le i \le N-t$, and $\rho'^{(t)}(i) = \rho'^{(t-1)}(i)$ for all $1 \le i \le N-t$. The induction hypothesis for $t-1$ now leads to (18), (19) for t.

CASE 2: $i_0 \in \Big(I_1(\rho) \cup I_2(\rho) \cup I_4(\rho)\Big) \cap [1, N-t]$. By the induction hypothesis, we have $\rho^{(t-1)}(i_0) = \rho'^{(t-1)}(i_0) = N-t+1$. The sorting process gives then $\rho^{(t)}(i_0) = \rho^{(t-1)}(N-t+1)$, and $\rho^{(t)}(i) = \rho^{(t-1)}(i)$ for $i \in \{1, 2, \ldots, N-t\} - \{i_0\}$. It also gives $\rho'^{(t)}(i_0) = \rho'^{(t-1)}(N-t+1)$, and $\rho'^{(t)}(i) = \rho'^{(t-1)}(i)$ for $i \in \{1, 2, \ldots, N-t\} - \{i_0\}$. As in case 1, it follows from the above equations and the induction hypothesis that (18) and (19) are true for t.

CASE 3: $i_0 = j_r \in I_3(\rho)$. In this case, we have, by the induction hypothesis, $\rho^{(t-1)}(j_s) = \rho'^{(t-1)}(j_{\sigma_3(s)})$ for $1 \le s \le m - \ell$. Thus, $\rho^{(t-1)}\Big(j_{\sigma_3^{-1}(r)}\Big) = \rho'^{(t-1)}(j_r) = N-t+1$. The sorting process dictates that $\rho^{(t)}\Big(j_{\sigma_3^{-1}(r)}\Big) = \rho^{(t-1)}(N-t+1)$, and $\rho'^{(t)}(j_r) = \rho'^{(t-1)}(N-t+1)$. Since $N-t+1 \in I_2(\rho) \cup I_4(\rho)$, we have by induction hypothesis, $\rho^{(t-1)}(N-t+1) = \rho'^{(t-1)}(N-t+1)$, and hence,

$$\rho^{(t)}\Big(j_{\sigma_3^{-1}(r)}\Big) = \rho'^{(t)}(j_r) \ . \tag{20}$$

Observe that the sorting process also lead to

$$\rho^{(t)}(i) = \rho^{(t-1)}(i) \quad \text{for} \quad i \in \{1, 2, \ldots, N-t\} - \Big\{j_{\sigma_3^{-1}(r)}\Big\} \quad \text{and} \tag{21}$$

$$\rho'^{(t)}(i) = \rho'^{(t-1)}(i) \quad \text{for} \quad i \in \{1, 2, \ldots, N-t\} - \{j_r\} \ . \tag{22}$$

We can establish (18), (19) for t by using (20), (21), (22) and the induction hypothesis for $t-1$.

This completes the inductive proof of (18) and (19), and thus the proof of Fact 3.

From Fact 3, we have with $t = m$, $\rho^{(m)}(j_s) = \rho'^{(m)}(j_{\sigma_3(s)})$ for $1 \le s \le m - \ell$. From Fact 1, we have $\rho'^{(m)}(j_{\sigma_3(s)}) = k_{\zeta(\sigma_3(s))}$. Therefore, we obtain

$$\rho^{(m)}(j_s) = k_{\zeta(\sigma_3(s))} \qquad \text{for } 1 \le s \le m - \ell.$$

This last equation, together with the fact $\rho^{(m)}(i) = \rho'^{(m)}(i)$ for $i \notin \{j_1, j_2, \cdots, j_{m-\ell}\}$ (Fact 3), shows that $\rho^{(m)} = b(\xi_{13}, \eta_{12}, \sigma_1, \zeta\sigma_3)$ The proof of Lemma 13 is now complete. □

Example 4 To illustrate the proof in the above lemma. Let $N = 9$, $m = 4$, and consider the $\rho = (3,9,5,6,7,8,4,1,2)$ in Example 3. Then $\rho' = (3,6,5,7,9,8,4,1,2)$ and $\rho'^{(m)} = (3,1,5,4,2)$. Note that $I_3(\rho) = \{2,4,5\}$, and thus the array $\rho'^{(m)}$ restricted to positions in $I_3(\rho)$ is $\beta = (1,4,2)$. This gives $\zeta = u(\xi_{24}, \eta_{34}, \sigma_2, \sigma_4) = \tau(\beta) = (1,3,2)$. As $\sigma_3 = (3,1,2)$, we have $\zeta\sigma_3 = (2,1,3)$, and thus $b(\xi_{13}, \eta_{12}, \sigma_1, \zeta\sigma_3) = (3,2,5,1,4)$. Lemma 13 asserts that $\rho^{(m)} = b(\xi_{13}, \eta_{12}, \sigma_1, \zeta\sigma_3)$. It is easy to verify that this is indeed true, by performing on $(3,9,5,6,7,8,4,1,2)$ m phases of the straight selection sort to obtain $\rho^{(m)}$.

Lemma 14 If $\xi_{13}, \eta_{12}, \sigma_1, \zeta$ are independently and uniformly chosen from their respective domains, then $b(\xi_{13}, \eta_{12}, \sigma_1; \zeta)$ is uniformly distributed over Σ_{N-m}.

Proof. Let ρ' be any element of Σ_{N-m}. For any choice of (ξ_{13}, η_{12}), there exists a unique pair (σ_1, ζ) such that $b(\xi_{13}, \eta_{12}, \sigma_1, \zeta) = \rho'$. Thus, the number of quadruples $(\xi_{13}, \eta_{12}, \sigma_1, \zeta)$ that are mapped by b to ρ' is equal to $\binom{N-m}{N-2m+\ell}^2$, a constant independent of ρ'. This proves the lemma. □

We will now establish (13), which implies (12) as mentioned at the beginning of this subsection. Consider first the case $i = 2$. Let r_ℓ denote the probability that a random $\rho' \in \Sigma_N$ will satisfy $|I_4(\rho')| = \ell$. Writing χ_δ as ρ, we have

$$E(R_2\, C_{N,m+1}) = \sum_{0 \le \ell \le m} r_\ell \frac{1}{|\Delta_{N,m,\ell}|} \sum_{\delta \in \Delta_{N,m,\ell}} |R_{\rho,2}||R_{\rho^{(m)}}| \ . \tag{23}$$

Now, from Lemmas 11, 12 and 13, we have

$$\frac{1}{|\Delta_{N,m,\ell}|} \sum_{\delta \in \Delta_{N,m,\ell}} |R_{\rho,2}| \cdot |R_{\rho^{(m)}}| = \frac{1}{|\Gamma_{m-\ell,\ell}|^2 |\Sigma_{m-\ell}|\, |\Sigma_\ell|} \sum_{\xi_{24},\eta_{34},\sigma_2,\sigma_4} v(\xi_{24}, \sigma_2, \sigma_4)$$

$$\times \left\{ \frac{1}{|\Gamma_{N-2m+\ell,m-\ell}|^2\, |\Sigma_{N-2m+\ell}|\, |\Sigma_{m-\ell}|} \sum_{\xi_{13},\eta_{12},\sigma_1,\sigma_3} \left| R_{b(\xi_{13},\eta_{12},\sigma_1,u(\xi_{24},\eta_{34},\sigma_2,\sigma_4)\sigma_3)} \right| \right\}.$$

By Lemma 14, the last factor multiplying $v(\xi_{24}, \sigma_2, \sigma_4)$ in the above expression is equal to $E(R_{\rho'})$ for a uniform random $\rho' \in \Sigma_{N-m}$. Thus, we obtain

$$\begin{aligned} &\frac{1}{|\Delta_{N,m,\ell}|} \sum_{\delta \in \Delta_{N,m,\ell}} |R_{\rho,2}||R_{\rho^{(m)}}| \\ &\qquad = \frac{1}{|\Gamma_{m-\ell,\ell}|^2 |\Sigma_{m-\ell}|\, |\Sigma_\ell|} \sum_{\xi_{24},\eta_{34},\sigma_2,\sigma_4} v(\xi_{24}, \sigma_2, \sigma_4)\, E(C_{N,m+1}) \\ &\qquad = E(C_{N,m+1}) \frac{1}{|\Delta_{N,m,\ell}|} \sum_{\delta \in \Delta_{N,m,\ell}} |R_{\rho,2}| \ . \end{aligned} \tag{24}$$

From (23) and (24) we have

$$\begin{aligned} E(R_2 C_{N,m+1}) &= E(C_{N,m+1}) \sum_{0 \le \ell \le m} r_\ell \frac{1}{|\Delta_{N,m,\ell}|} \sum_{\delta \in \Delta_{N,m,\ell}} |R_{\chi_\delta,2}| \\ &= E(C_{N,m+1}) E(R_2) \ . \end{aligned} \quad (25)$$

In a similar way, one can prove

$$E(R_4 C_{N,m+1}) = E(C_{N,m+1}) E(R_4). \quad (26)$$

It remains to prove (13) for the case $i = 3$. By Lemma 9,

$$\left|R_{\rho^{-1},3}\right| = \left|R_{\rho,2}\right| \quad (27)$$

It follows that

$$E(R_3) = E(R_2) \quad (28)$$

To evaluate the expression $E(R_3 C_{N,m+1})$, we take a random uniform $\rho \in \Sigma_N$ and calculate the expected value of $|R_{\rho^{-1},3}| \cdot |R_{(\rho^{-1})^{(m)}}|$. By Lemma 1, 2, 3, 5, 6, we have

$$\begin{aligned} \left|R_{(\rho^{-1})^m}\right| &= \left|MAX\left(V((\rho^{-1})^{(m)})\right)\right| \\ &= \left|MAX\left(d^{(m)}\left(V(\rho^{-1})\right)\right)\right| \\ &= \left|MAX\left(d^{(m)}\left(\text{dual}(V(\rho))\right)\right)\right| \\ &= \left|MAX\left(\text{dual}\left(d^{(m)}(V(\rho))\right)\right)\right| \\ &= \left|MAX\left(d^{(m)}(V(\rho))\right)\right| \\ &= \left|MAX\left(V(\rho^{(m)})\right)\right| \\ &= \left|R_{\rho^{(m)}}\right| \ . \end{aligned} \quad (29)$$

From (27) and (29), we have

$$E(R_3 C_{N,m+1}) = E(R_2 C_{N,m+1}) \ . \quad (30)$$

It follows from (25), (28) and (30) that $E(R_3 C_{N,m+1}) = E(C_{N,m+1}) E(R_3)$. This proves (13) for the case $i = 3$. We have established (12).

Remark Geometrically, the case $i = 3$ is *dual* to the case $i = 2$. If one developes the duality aspect a little deeper than we have done, then the present proof for the case $i = 3$ will not be needed.

3.4 Second Step

In this subsection, we will prove

$$E(R_1) = E(r_{N,m,5}) \ , \tag{31}$$

and

$$E(R_1\, C_{N,m+1}) = E(r_{N,m,5}\, r_{N,m,1}) \ . \tag{32}$$

This will complete the proof of Theorem 1, since (8) is clearly a consequence of (12), (31), and (32).

Lemma 15 Let $\rho \in \Sigma_N$. If $D_4(V(\rho)) = \emptyset$, then

$$\left|R_{\rho,1}\right| = \left|MAX\Big(D_5(V(\rho))\Big)\right| \ .$$

Proof. Let $S = V(\rho)$. By Lemma 8,

$$|R_{\rho,1}| = |D_1(S) \cap MAX(S)| \ . \tag{33}$$

We now prove

$$D_1(S) \cap MAX(S) = MAX(D_5(S)) \ . \tag{34}$$

Clearly (33) and (34) imply the lemma.

Note that S is a standard set. Since $D_4(S) = \emptyset$, we have $|D_2(S)| = |D_3(S)| = m > 0$. Let $(x_i, y_i) \in D_2(S)$ with $y_i = \max\{z' \mid (z, z') \in D_2(S)\}$, and $(x_j, y_j) \in D_3(S)$ with $x_j = \max\{z \mid (z, z') \in D_3(S)\}$. Then any point in $D_1(S) - D_5(S)$ will be dominated by either (x_i, y_i) or (x_j, y_j), and cannot be in $MAX(S)$. This proves $D_1(S) \cap MAX(S) \subseteq MAX(D_5(S))$. On the other hand, any point (z, z') in $MAX(D_5(S))$ must satisfy $z > x_j$ and $z' > y_i$, and therefore cannot be dominated by any point in either $D_2(S)$ or $D_3(S)$. This proves $D_1(S) \cap MAX(S) \supseteq MAX(D_5(S))$. This proves (34) and the lemma. □

Lemma 16 If $D_5(V(\rho)) \neq \emptyset$, then $MAX\Big(d^{(m)}(V(\rho))\Big) = MAX\Big(D_1(V(\rho))\Big)$.

Proof. Let $S = V(\rho)$ and v be any point of $D_5(S)$. Since $D_5(S) \neq \emptyset$, we have $D_4(S) = \emptyset$. Suppose $D_2(S) = \{(x_{i_s}, y_{i_s}) \mid 1 \le s \le m\}$ with $x_{i_1} > x_{i_2} > \ldots > x_{i_m}$, and $D_3(S) = \{(x_{j_t}, y_{j_t}) \mid 1 \le t \le m\}$ with $y_{j_1} > y_{j_2} > \ldots > y_{j_m}$. Then, from the definition of d, it is easy to see that $d^{(m)}(S) = D_1(S) \cup \{(x_{j_s}, y_{i_s}) \mid 1 \le s \le m\}$. Since each (x_{j_s}, y_{i_s}) is clearly dominated by v, we have $MAX(d^{(m)}(S)) = MAX(D_1(S))$. □

We now prove (31). Let $\Sigma'_N = \{\rho \mid \rho \in \Sigma_N,\ D_4(V(\rho)) = \emptyset\}$. Clearly, if $|R_{\rho,1}| \neq 0$, then $\rho \in \Sigma'_N$. By Lemma 15, we have thus

$$\begin{aligned} E(R_1) &= \frac{1}{N!} \sum_{\rho \in \Sigma'_N} |R_{\rho,1}| \\ &= \frac{1}{N!} \sum_{\rho \in \Sigma'_N} \left| MAX\left(D_5(V(\rho))\right)\right| . \end{aligned}$$

As $D_5(V(\rho)) = \emptyset$ for $\rho \in \Sigma_N - \Sigma'_N$, we have

$$E(R_1) = \frac{1}{N!} \sum_{\rho \in \Sigma_N} \left| MAX\left(D_5(V(\rho))\right)\right| . \tag{35}$$

For any standard N-set $S = \{(x_1, y_1), (x_2, y_2), \ldots, (x_N, y_N)\}$ with $x_1 < x_2 < \ldots < x_N$, let $type(S)$ denote the permutation $\sigma \in \Sigma_N$ such that y_j is the $\sigma(j)$-th smallest element among $y_1, y_2, \ldots, y_N$. Then $|MAX(D_5(S))| = |MAX(D_5(V(\sigma)))|$, where $\sigma =$ type (S). Since, for a uniform random N-set S, type (S) is equally likely to be any $\sigma \in \Sigma_N$, equation (35) implies that $E(R_1)$ is the expected value of $MAX(D_5(S))$ for a random uniform N-set S. That is,

$$E(R_1) = E(r_{N,m,5}) .$$

This proves (31).

To prove (32), we use Lemma 1 and Lemma 2 to obtain

$$\begin{aligned} E(R_1\, C_{N,m+1}) &= \frac{1}{N!} \sum_{\rho \in \Sigma'_N} |R_{\rho,1}| \cdot |R_{\rho(m)}| \\ &= \frac{1}{N!} \sum_{\rho \in \Sigma'_N} |R_{\rho,1}| \cdot |MAX(V(\rho^{(m)}))| \\ &= \frac{1}{N!} \sum_{\rho \in \Sigma'_N} |R_{\rho,1}| \cdot \left| MAX\left(d^{(m)}(V(\rho))\right)\right| . \end{aligned}$$

We then use Lemma 15 and Lemma 16 to get

$$\begin{aligned} E(R_1\, C_{N,m+1}) &= \frac{1}{N!} \sum_{\rho \in \Sigma'_N} \left| MAX\left(D_5(V(\rho))\right)\right| \cdot \left| MAX\left(d^{(m)}(V(\rho))\right)\right| \\ &= \frac{1}{N!} \sum_{\rho \in \Sigma'_N} \left| MAX\left(D_5(V(\rho))\right)\right| \cdot \left| MAX\left(D_1(V(\rho))\right)\right| . \end{aligned} \tag{36}$$

As in the derivation of (31), we infer from (36) that $E(R_1\, C_{N,m+1})$ is the expected value of $|MAX(D_5(S))| \cdot |MAX(D_1(S))|$ for a uniform random N-set S. That is,

$$E(R_1\, C_{N,m+1}) = E(r_{N,m,5}\, r_{N,m,1}) .$$

This proves (32), and completes the proof of Theorem 1.

4 Proof of Theorem 2

In this section we will assume that $N \geq 2m$; otherwise Theorem 2 is clearly true, as $p_{N,m} = 0$ and the random variable $r_{N,m,5}$ is identically 0.

Let $S = \{v_j \mid v_j = (x_j, y_j),\ 1 \leq j \leq N\}$ be any standard N-set in the unit square, and $D_i(S)$, $1 \leq i \leq 5$, are defined (with respect to m) as in Section 1. We introduce two more definitions. Let $D_6(S) = D_7(S) = \emptyset$ if $D_5(S) = \emptyset$. Otherwise, let $D_6(S) = (D_1(S) - D_5(S)) \cap ([0,1] \times [b,1])$ and $D_7(S) = (D_1(S) - D_5(S)) \cap ([c,1] \times [0,1])$, where $b = \max\{y_k \mid v_k \in D_5(S)\}$ and $c = \max\{x_{k'} \mid v_{k'} \in D_5(S)\}$ (see Figure 4).

Lemma 17 If $D_5(S) \neq \emptyset$, then $MAX(D_1(S))$ is the disjoint union of $MAX(D_i(S))$, $i \in \{5,6,7\}$.

Proof. Let $v_s, v_t \in D_5(S)$ be such that $y_s = \max\{y_k \mid v_k \in D_5(S)\}$ and $x_t = \max\{x_{k'} \mid v_{k'} \in D_5(S)\}$; s and t may be the same.

First we prove that $MAX(D_1(S)) \subseteq \cup_{i\in\{5,6,7\}} MAX(D_i(S))$. Suppose that $v_j \in MAX(D_1(S))$. If $x_j > x_t$, then $v_j \in (D_1(S) - D_5(S)) \cap ([x_t, 1] \times [0,1]) = D_7(S)$. If $y_j > y_s$, then $v_j \in (D_1(S) - D_5(S)) \cap ([0,1] \times [y_s, 1]) = D_6(S)$. If $x_j \leq x_t$ and $y_j \leq y_s$, then we must have $y_j > y_t$ and $x_j > x_s$, since otherwise, v_j will be dominated by either v_s or v_t; this implies that, in this case, $v_j \in D_1(S) \cap ([x_s, 1] \times [y_t, 1]) \subseteq D_5(S)$. Thus, we have proved that $MAX(D_1(S)) \subseteq \cup_{i\in\{5,6,7\}} D_i(S)$, which implies immediately $MAX(D_1(S)) \subseteq \cup_{i\in\{5,6,7\}} MAX(D_1(S))$.

Next, we observe that if $v_j \in D_i(S)$, where $i \in \{5,6,7\}$, and $v_{j'} \in D_1(S) - D_i(S)$, then v_j cannot be dominated by $v_{j'}$. This implies that any v_j in $MAX(D_i(S))$ must also be a maximal point in $D_1(S)$. That is, $MAX(D_i(S)) \subseteq MAX(D_1(S))$ for $i \in \{5,6,7\}$. Hence, $\cup_{i\in\{5,6,7\}} MAX(D_i(S)) \subseteq MAX(D_1(S))$.

The above discussion proves that $MAX(D_1(S)) = \cup_{i\in\{5,6,7\}} MAX(D_1(S))$. As $MAX(D_i(S))$, $i \in \{5,6,7\}$, are disjoint, we have completed the proof of Lemma 17.□

Take a uniform random N-set S, and let $r_{N,m,6}$, $r_{N,m,7}$ denote the random variables that take on the values $|MAX(D_6(S))|$, $|MAX(D_7(S))|$, respectively. It follows from Lemma 17 that

$$\begin{aligned} E(r_{N,m,5}\, r_{N,m,1}) &= E\Big(r_{N,m,5}(r_{N,m,5} + r_{N,m,6} + r_{N,m,7})\Big) \\ &= E(r_{N,m,5}^2) + E(r_{N,m,5}\, r_{N,m,6}) + E(r_{N,m,5}\, r_{N,m,7}) \ . \end{aligned} \tag{37}$$

Lemma 18 $E(r_{N,m,5}\, r_{N,m,7}) = E(r_{N,m,5}\, r_{N,m,6})$.

Proof. For any standard N-set S, we have

$$D_5(\text{dual}(S)) = \text{dual}(D_5(S)) \ , \tag{38}$$

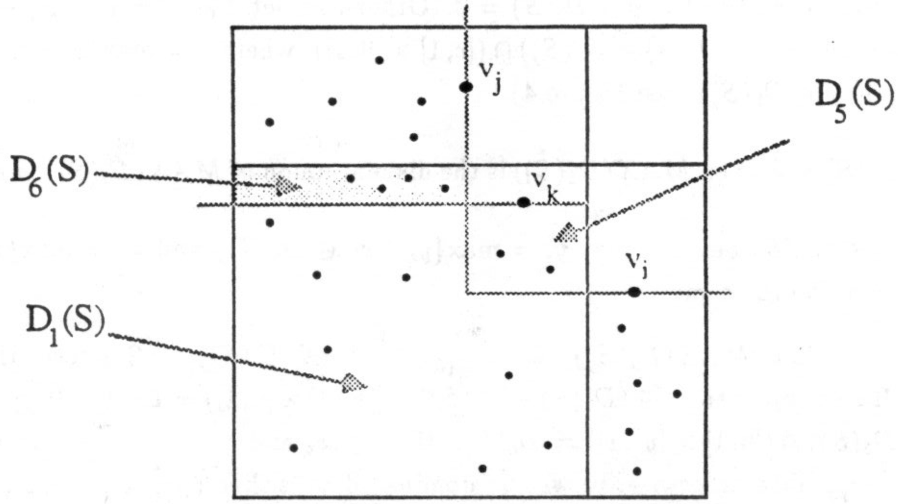

Figure 4: Illustration of $D_6(S)$

and

$$D_7(\text{dual}(S)) = \text{dual}(D_6(S)) \ . \tag{39}$$

Formula (38) follows from Lemma 5. The proof of (39) is straightforward.

If we generate a uniform random N-set S, then dual(S) is also a uniform random N-set. Thus, $E(r_{N,m,5}\, r_{N,m,7})$ is the expected value of $\left|MAX\left(D_5(\text{dual}(S))\right)\right| \cdot \left|MAX\left(D_7(\text{dual}(S))\right)\right|$, which by (38) and (39) is equal to $\left|MAX\left(\text{dual}(D_5(S))\right)\right| \cdot \left|MAX\left(\text{dual}(D_6(S))\right)\right| = |MAX(D_5(S))| \cdot |MAX(D_6(S))|$. This clearly implies that $E(r_{N,m,5}\, r_{N,m,7}) = E(r_{N,m,5}\, r_{N,m,6})$. □

From (37) and Lemma 18, we obtain

$$E(r_{N,m,5}\, r_{N,m,1}) = E(r_{N,m,5}^2) + 2E(r_{N,m,5}\, r_{N,m,6}) \ . \tag{40}$$

We will derive formulas for $E(r_{N,m,5})$, $E(r_{N,m,5}^2)$ and $E(r_{N,m,5}\, r_{N,m,6})$, and then use (40) to complete the proof of Theorem 2.

Let $\mathcal{F}_N$ be the family of all sets of the form $S = \{(x_i, y_i) \mid 1 \le i \le N,\ 0 \le x_i, y_i \le 1\}$. Let F be a real-valued function on $\mathcal{F}_N$ satisfying the conditions (a) for all S, $|F(S)| < c$ where $c > 0$ is some constant, and (b) if S is a standard N-set and $D_4(S) = \emptyset$, then $F(S) = 0$. Now, take a uniform random N-set S, and let Y denote the random variable which takes on the value $F(S)$. Also, let d_i, $1 \le i \le 7$, denote the random variables that take on the value $|D_i(S)|$ if S is a standard N-set, and a constant value $c = 0$ otherwise. (In fact, c can be chosen to be any constant for our purpose, as S will be a standard N-set with probability 1.) Clearly,

$$E(Y) = \Pr\{d_4 = 0\} \sum_{k \ge 0} \Pr\{d_5 = k \mid d_4 = 0\} \cdot E(Y \mid d_4 = 0,\ d_5 = k) \ , \tag{41}$$

and

$$E(Y) = \Pr\{d_4 = 0\} \sum_{k \ge 0} \sum_{\ell \ge 0} \Pr\{d_5 = k,\ d_6 = \ell \mid d_4 = 0\} \cdot E(Y \mid d_4 = 0,\ d_5 = k,\ d_6 = \ell) \ . \tag{42}$$

Lemma 19 $\Pr\{d_4 = 0\} = p_{N,m}$.

Proof. In the calculation, we can ignore the possibility that S is not a standard N-set, since that occurs with probability 0. If S is a standard N-set, then $|D_4(S)| = 0$ if and only if $I_4(\text{type}(S)) = \emptyset$. It follows that $\Pr\{d_4 = 0\}$ is equal to the fraction of $\rho \in \Sigma_N$ with $I_4(\rho) = \emptyset$. Now, one can assign to each ρ satisfying $I_4(\rho) = \emptyset$ a unique $(m+1)$-tuple $(i_1, i_2, \ldots, i_m; \sigma)$ such that (a) $i_1, i_2, \ldots, i_m$ are distinct integers in the range $[1,\ N-m]$, (b) $\sigma \in \Sigma_{N-m}$, (c) $\rho(N-s+1) = i_s$ for $1 \le s \le m$, and (d) $\sigma = \tau(\rho')$, where ρ' is the array ρ restricted to positions in $\{1, 2, \ldots, N-m\}$ (i.e. $\rho' \in \Sigma_{N-m}$ with $\rho'(j) = \rho(j)$). It is easy to see that this assignment is a one-to-one and onto mapping between the set of ρ satisfying $I_4(\rho) = \emptyset$ and the set of all $(m+1)$-tuples $(i_1, i_2, \ldots, i_m; \sigma)$ satisfying conditions (a), (b) above. Thus, the number of $\rho \in \Sigma_N$ satisfying $I_4(\rho) = \emptyset$ is equal to $\binom{N-m}{m} m!\,(N-m)!$. Hence, $\Pr\{d_4 = 0\}$ is equal to $\binom{N-m}{m} m!\,(N-m)!\,/N! = p_{N,m}$. □

Lemma 20 $\Pr\{d_5 = k \mid d_4 = 0\} = \int_0^1 \int_0^1 h_{N,m}(\lambda, \lambda', k) d\lambda\, d\lambda'$, for all integers $k \geq 0$.

Proof. Let $a_k = \Pr\{d_5 = k \mid d_4 = 0\}$. Since only type (S), which represents the relative ordering of the coordinates of points in S, and not the scale, is relevant, we normalize $D_1(S)$ to occupy $[0,1] \times [0,1]$ and compute a_k accordingly. Consider the following random process:

(a) Generate independent random variables $y_1, y_2, \ldots, y_m$, each of which is uniformly distributed over $[0,1]$; let $y_{\max} = \max\{y_1, y_2, \ldots, y_m\}$;

(b) Generate independent random variables $x_1, x_2, \ldots, x_m$, each of which is uniformly distributed over $[0,1]$; let $x_{\max} = \max\{x_1, x_2, \ldots, x_m\}$;

(c) Generate $N - 2m$ independent random points $v_1, v_2, \ldots, v_{N-2m}$, each of which is uniformly chosen over the unit square $[0,1] \times [0,1]$.

We will interprete the above random process as follows: $\{v_1, v_2, \cdots, v_{N-2m}\}$ is the set $D_1(S)$, the y_i's are the y-coordinates of the points in $D_2(S)$, and the x_i's are the x-coordinates of the points in $D_3(S)$. Now, let $J_{N,m,k}$ be the event that exactly k points v_i are in $[x_{\max}, 1] \times [y_{\max}, 1]$. Clearly $a_k = \Pr\{J_{N,m,k}\}$, as we can identify $D_1(S)$ with $\{v_1, v_2, \ldots, v_{N-2m}\}$, and $D_5(S)$ with those v_i in $[x_{\max}, 1] \times [y_{\max}, 1]$.

Let $\lambda = 1 - x_{\max}$, $\lambda' = 1 - y_{\max}$. To calculate $\Pr\{J_{N,m,k}\}$, we note that the probability density for (λ, λ') is given by $\rho(\lambda, \lambda') = m^2(1-\lambda)^{m-1}(1-\lambda')^{m-1}$ for $0 < \lambda,\ \lambda' < 1$. The probability that exactly k v_i fall into the region $[1-\lambda,\ 1] \times [1-\lambda',\ 1]$ (see Figure 5) is equal to $\binom{N-2m}{k}(\lambda\lambda')^k(1-\lambda\lambda')^{N-2m-k}$. Thus,

$$\begin{aligned}
\Pr\{J_{N,m,k}\} &= \int_0^1 \int_0^1 \rho(\lambda, \lambda') \binom{N-2m}{k} (\lambda\lambda')^k (1-\lambda\lambda')^{N-2m-k}\, d\lambda\, d\lambda' \\
&= \int_0^1 \int_0^1 h_{N,m}(\lambda, \lambda', k)\, d\lambda\, d\lambda' .
\end{aligned}$$

This proves Lemma 20. □

We adopt the convention that $H_0 = H_0^{(2)} = 0$.

Lemma 21 For all integers $k \geq 0$, $E(r_{N,m,5} \mid d_4 = 0, d_5 = k) = H_k$, and $E(r_{N,m,5}^2 \mid d_4 = 0, d_5 = k) = H_k^2 + H_k - H_k^{(2)}$.

Proof. Clearly the lemma is true for $k = 0$. Now, let $k > 0$. As in the proof of Lemma 20, we can compute the expected value and variance of $r_{N,m,5}$ by using the distribution generated as in the proof of Lemma 20, conditioned on the occurrence of event $J_{N,m,k}$. When $J_{N,m,k}$ occurs with parameter values λ, λ', the k points $v_{i_1}, v_{i_2}, \ldots, v_{i_k}$ that fall in the region $[1-\lambda,\ 1] \times [1-\lambda',\ 1]$ are independently and uniformly distributed over that region (see Figure 5). Thus, $E(r_{N,m,5} \mid$

$d_4 = 0,\ d_5 = k) = E(C_{k,1}) = H_k$, and $E(r^2_{N,m,5} \mid d_4 = 0,\ d_5 = k) = E(C^2_{k,1}) = \left(E(C_{k,1})\right)^2 + Var(C_{k,1}) = H_k^2 + H_k - H_k^{(2)}$, where we have used (2) and (3) in the derivation. □

Lemma 22 For all integers $k \geq 1$ and $\ell \geq 0$, $\Pr\{d_5 = k,\ d_6 = \ell \mid d_4 = 0\} = \int_0^1 \int_0^1 \int_0^1 h_{N,m}(\lambda, \lambda', k)\, q_{N,m,k,\ell}(\lambda, \lambda', k)\, d\lambda\, d\lambda'\, dz$.

Proof. Let $a_{k,\ell} = \Pr\{d_5 = k,\ d_6 = \ell \mid d_4 = 0\}$. We consider the following process:

(a) Generate independent random variables $y_1, y_2, \ldots, y_m$, each of which is uniformly distributed over $[0,1]$; let $y_{\max} = \max\{y_1, y_2, \ldots, y_m\}$;

(b) Generate independent random variables $x_1, x_2, \ldots, x_m$, each of which is uniformly distributed over $[0,1]$; let $x_{\max} = \max\{x_1, x_2, \ldots, x_m\}$;

(c) Generate $N - 2m$ independent random points $v_i = (w_i, z_i)$, $1 \leq i \leq N - 2m$, each of which is uniformly chosen from the unit square $[0,1] \times [0,1]$;

(d) Let $r = 0$ if there is no v_i in $[1 - x_{\max},\ 1] \times [1 - y_{\max},\ 1]$, and otherwise, let $r = 1 - \max\{z_i \mid v_i \in [1 - x_{\max},\ 1] \times [1 - y_{\max},\ 1]\}$.

Let $J_{N,m,k,\ell}$ be the event that exactly k points are in the region $[x_{\max},\ 1] \times [y_{\max},\ 1]$, and exactly ℓ points are in the region $[0, x_{\max}] \times [1 - r,\ 1]$. An interpretation of the above random process similar to that used in the proof of Lemma 21 gives $a_{k,\ell} = \Pr\{J_{N,m,k,\ell}\}$.

Let $\lambda = 1 - x_{\max}$ and $\lambda' = 1 - y_{\max}$. To compute $\Pr\{J_{N,m,k,\ell}\}$ for $k \geq 1$, $\ell \geq 0$, observe that the probability density for (λ, λ', r) is given by $\rho(\lambda, \lambda', r) = m^2(1-\lambda)^{m-1}(1-\lambda')^{m-1}(N - 2m)\lambda(1-\lambda r)^{N-2m-1}$, for $0 < \lambda,\ \lambda' < 1$ and $0 < r < \lambda'$. Now, let $C_{\lambda,\lambda',r}(k,\ell)$ be the probability that, given (λ, λ', r), exactly $k - 1$ v_i fall into the region $F_1 \equiv [1 - \lambda,\ 1] \times [1 - \lambda',\ 1 - r]$, and exactly ℓ v_j fall into the region $F_2 \equiv [0, 1 - \lambda] \times [1 - \lambda', 1]$. (See Figure 6.) Then,

$$C_{\lambda,\lambda',r}(k,\ell) = \binom{N-2m-1}{k-1} \left(\frac{\lambda(\lambda' - r)}{1 - \lambda r}\right)^{k-1} \binom{N-2m-k}{\ell} \times \left(\frac{r(1-\lambda)}{1-\lambda r}\right)^{\ell} \left(\frac{1 - \lambda\lambda' - r(1-\lambda)}{1 - \lambda r}\right)^{N-2m-k-\ell} .$$

Thus,

$$\begin{aligned}
\Pr\{J_{N,m,k,\ell}\} &= \int_0^1 \int_0^1 \int_0^{\lambda'} \rho(\lambda, \lambda', r)\, C_{\lambda,\lambda',r}(k,\ell)\, dr\, d\lambda'\, d\lambda \\
&= \int_0^1 \int_0^1 \int_0^1 \rho(\lambda, \lambda', \lambda' z)\, C_{\lambda,\lambda',\lambda' z}(k,\ell) \lambda'\, dz\, d\lambda'\, d\lambda \\
&= \int_0^1 \int_0^1 \int_0^1 h_{N,m}(\lambda, \lambda', k)\, q_{N,m,k,\ell}(\lambda, \lambda', z)\, dz\, d\lambda'\, d\lambda .
\end{aligned}$$

This proves Lemma 22. □

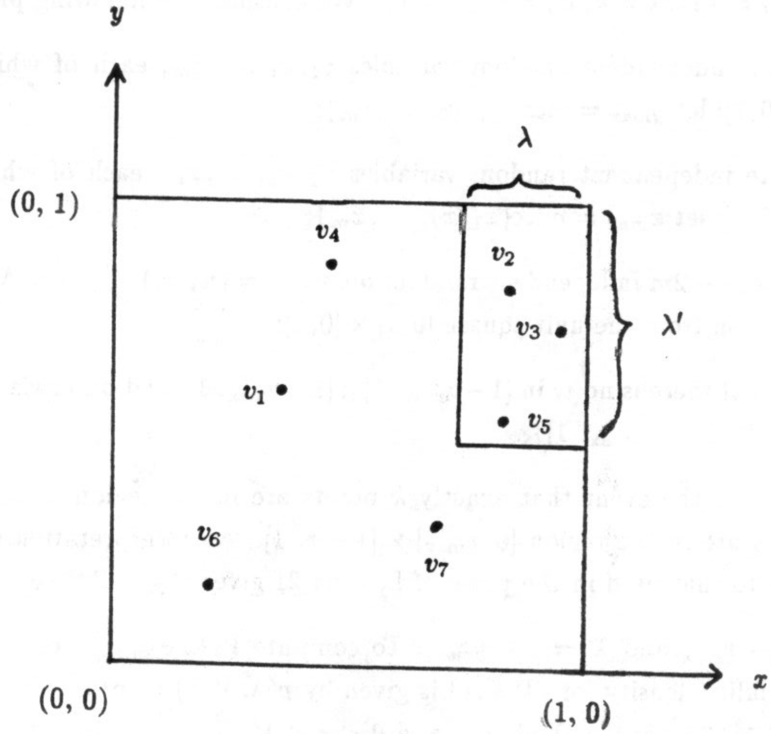

Figure 5: Normalized representation of $D_1(S)$; $N - 2m = 7$.
Event $J_{N,m,3}$ occurs in this case.

Lemma 23 $E(r_{N,m,5}\, r_{N,m,6} \mid d_4 = 0,\ d_5 = k,\ d_6 = \ell) = H_k\, H_\ell$, for all integers $k, \ell \geq 0$.

Proof. This lemma is clearly true for either $k = 0$ or $\ell = 0$. Now suppose $k, \ell > 0$. We can compute the expected value of $r_{N,m,5}\, r_{N,m,6}$ by using the distribution generated as in the proof of Lemma 22, conditioned on the occurrences of the event $J_{N,m,k,\ell}$. Suppose $J_{N,m,k,\ell}$ occurs with λ, λ', r being the parameter values as described in the proof of Lemma 22; let $v_{i_1}, v_{i_2}, \ldots, v_{i_k}$ be the k points in the region $[1-\lambda,\ 1] \times [1-\lambda', 1]$, such that v_{i_1} is on the horizontal line segment L_0 joining the point $(1-\lambda,\ 1-r)$ to the point $(1,\ 1-r)$, and $v_{i_2} \ldots, v_{i_k}$ are in the region F_1; let $v_{j_1}, v_{j_2}, \ldots, v_{j_\ell}$ be the points in the region F_2. (See Figure 6.)

The probability distribution K_1 of $(v_{i_1}, v_{i_2}, \ldots, v_{i_k})$ can be described by picking v_{i_1} uniformly on the segment L_0, and picking each of $v_{i_2}, v_{i_3}, \ldots, v_{i_k}$ independently and uniformly over L_1; the probability distribution K_2 of $(v_{j_1}, v_{j_2}, \ldots, v_{j_\ell})$ can be obtained by picking each of $v_{j_1}, v_{j_2}, \ldots, v_{j_\ell}$ independently and uniformly over L_2. Furthermore, K_1 and K_2 are independent of each other. This implies that $E(r_{N,m,5}\, r_{N,m,6} \mid d_4 = 0,\ d_5 = k,\ d_6 = \ell) = E(C_{k,1})\, E(C_{\ell,1}) = H_k\, H_\ell$. □

It follows from (41), and Lemmas 19, 20 and 21 that

$$\begin{aligned} E(r_{N,m,5}) &= p_{N,m} \sum_{k \geq 0} H_k \int_0^1 \int_0^1 h_{N,m}(\lambda, \lambda', k)\, d\lambda\, d\lambda' \\ &= p_{N,m} \sum_{k \geq 1} H_k \int_0^1 \int_0^1 h_{N,m}(\lambda, \lambda', k)\, d\lambda\, d\lambda' \ , \end{aligned} \tag{43}$$

and also

$$\begin{aligned} E\left(r_{N,m,5}^2\right) &= p_{N,m} \sum_{k \geq 0} \left(H_k^2 + H_k - H_k^{(2)}\right) \int_0^1 \int_0^1 h_{N,m}(\lambda, \lambda', k)\, d\lambda\, d\lambda' \\ &= p_{N,m} \sum_{k \geq 1} \left(H_k^2 + H_k - H_k^{(2)}\right) \int_0^1 \int_0^1 h_{N,m}(\lambda, \lambda', k)\, d\lambda\, d\lambda' \ . \end{aligned} \tag{44}$$

Similarly, it follows from (42), Lemmas 19, 22 and 23 that

$$E(r_{N,m,5}\, r_{N,m,6}) =$$
$$p_{N,m} \sum_{k \geq 1} \sum_{\ell \geq 1} H_k\, H_\ell \int_0^1 \int_0^1 \int_0^1 h_{N,m}(\lambda, \lambda', k)\, q_{N,m,k,\ell}(\lambda, \lambda', z)\, d\lambda\, d\lambda'\, dz \ . \tag{45}$$

Theorem 2 is an immediate consequence of (40), (43), (44) and (45).

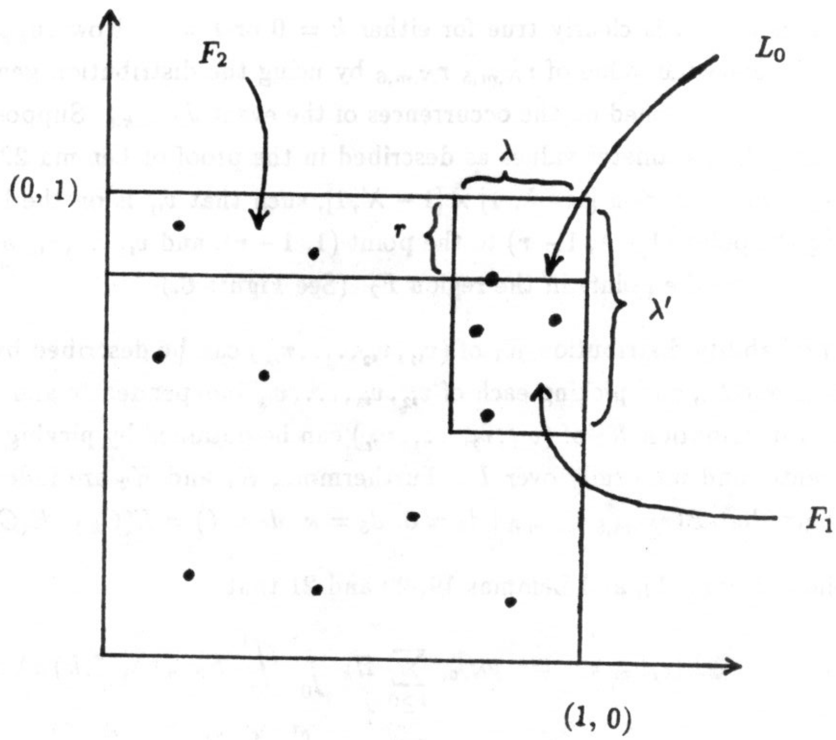

Figure 6: Normalized representation of $D_1(S)$, $D_5(S)$, and $D_6(S)$; Event $J_{N,m,4,2}$ occurs in this case.

5 Some Mathematical Formulas

We give in this section formulas which will be useful for the proof of Theorem 3. All proofs will be relegated to the Appendices. The constants in the O-notations for the rest of this paper will be absolute constants, unless otherwise specified.

Let $N_1 = N^{7/16}$, $N_2 = N^{1/2+\epsilon}$, where $\epsilon = 1/400$, $N_3 = N^{5/16}$, $a(m,N) = (10 \ln N)/m$, $b(m,N) = 1/(m\,N^{1/10})$, and γ be the Euler's constant $\lim_{k\to\infty} - \left(H(k) - \sum_{1\le i\le k} 1/i\right)$. It is well known (e.g. Knuth [K2, Section 1.2.11.2]) that $H(k) = \ln k + \gamma + O(1/k)$ for large k.

Definition 11 For $0 < \lambda, \lambda', z < 1$, $N > 0$, and $m,\ k \ge 0$, let

$$\hat{h}_{N,m}(\lambda,\lambda',k) = \frac{(\lambda\lambda' N)^k}{k!}\, e^{-\lambda\lambda' N}\, m^2\, e^{-(\lambda+\lambda')m} \quad .$$

Definition 12 For $x, u, v \ge 0$, $j \in \{0,1\}$, and integer $k \ge 1$, let

$$\psi_{j,k}(x,u,v) = \frac{(uv)^k}{k!}\, e^{-uv}\, x^2\, e^{-x^2-(u+v)x}\, (\ln v)^j \quad .$$

5.1 Formulas involving $p_{N,m}$ and $h_{N,m}$.

Lemma 24 For large N, $p_{N,m} = e^{-m^2/N}(1 + O(N^{-1/2+3\epsilon}))$ for $1 \le m < N_2$, and $p_{N,m} = O(e^{-N^{2\epsilon}})$ for $N_2 \le m \le N-2$.

Lemma 25 For any fixed integer $k \ge 0$, $\sum_{m\ge 1} m^k\, e^{-m^2/N} = O(N^{(k+1)/2})$ for large N. (The constants depend on k in this case.)

Lemma 26 For any $0 < \lambda,\ \lambda' < 1$, and $1 \le m \le N/2$, we have

$$\sum_{0\le k\le N-2m} h_{N,m}(\lambda,\lambda',k) = m^2(1-\lambda)^{m-1}(1-\lambda')^{m-1},$$

$$\sum_{0\le k\le N-2m} \int_0^1 \int_0^1 h_{N,m}(\lambda,\lambda',k)\, d\lambda\, d\lambda' = 1,$$

$$\sum_{k\ge 0} \hat{h}_{N,m}(\lambda,\lambda',k) = m^2\, e^{-(\lambda+\lambda')m},$$

and

$$\sum_{k\ge 0} \int_0^1 \int_0^1 \hat{h}_{N,m}(\lambda,\lambda',k)\, d\lambda\, d\lambda' \le 1 \quad .$$

Lemma 27 Let $N_1 \le m < N_2$, $1 \le k < N_3$, $\lambda \in (0,\ a(m,N))$, and $\lambda' \in (0,\ a(m,N))$. Then, for large N, $h_{N,m}(\lambda,\lambda',k) = (1 + O(N^{-1/8}))\, \hat{h}_{N,m}(\lambda,\lambda',k)$.

Lemma 28 For $N_1 \le m < N_2$, $1 \le k \le N-2m$, and let $f(\lambda,\lambda',k)$ stand for either $h_{N,m}(\lambda,\lambda',k)$ or $\hat{h}_{N,m}(\lambda,\lambda',k)$ we have, for large N,

$$\int_0^1\int_0^1 f(\lambda,\lambda',k)\,d\lambda\,d\lambda' = \int_0^{a(m,N)}\int_0^{a(m,N)} f(\lambda,\lambda',k)\,d\lambda\,d\lambda' + O(N^{-10}) \ .$$

Lemma 29 For $N_1 \le m < N_2$, $N_3 \le k \le N-2m$, and let $f(\lambda,\lambda',k)$ stand for either $h_{N,m}(\lambda,\lambda',k)$ or $\hat{h}_{N,m}(\lambda,\lambda',k)$, we have, for large N,

$$\int_0^1\int_0^1 f(\lambda,\lambda',k)\,d\lambda\,d\lambda' = O(N^{-10}) \ .$$

Lemma 30 Let $N_1 \le m < N_2$, and $F(k)$ be a function such that $|F(k)| = O((\log\,k)^2)$ for large k. Let $f(\lambda,\lambda',k)$ stand for either $h_{N,m}(\lambda,\lambda',k)$ or $\hat{h}_{N,m}(\lambda,\lambda',k)$. We have, for large N,

$$\sum_{1\le k<N_3}\int_0^{a(m,N)}\int_{b(m,N)}^{a(m,N)} F(k)\,f(\lambda,\lambda',k)\,d\lambda'\,d\lambda$$
$$= \sum_{1\le k<N_3}\int_0^1\int_0^1 F(k)\,f(\lambda,\lambda',k)\,d\lambda'\,d\lambda + O\Big(N^{-1/10}(\log\,N)^2\Big)$$

and,

$$\sum_{1\le k<N_3}\int_0^{a(m,N)}\int_{b(m,N)}^{a(m,N)} F(k)\,f(\lambda,\lambda',k)\,\ln(N\,\lambda')\,d\lambda'\,d\lambda$$
$$= \sum_{1\le k<N_3}\int_0^1\int_0^1 F(k)\,f(\lambda,\lambda',k)\,\ln(N\,\lambda')\,d\lambda'\,d\lambda + O\Big(N^{-1/10}(\log\,N)^3\Big) \ .$$

5.2 Formulas involving $q_{N,m,k,\ell}$

Lemma 31 For all $1 \le m \le N/2$, $1 \le k \le N-2m$, and $0 < \lambda,\ \lambda' < 1$, we have

$$\sum_{\ell\ge 0} q_{N,m,k,\ell}(\lambda,\lambda',z) = k(1-z)^{k-1} \quad \text{for all } 0<z<1, \qquad \text{and}$$
$$\sum_{\ell\ge 0}\int_0^1 q_{N,m,k,\ell}(\lambda,\lambda',z)\,dz = 1 \ .$$

Lemma 32 Let $N_1 \le m < N_2$, and $F(k,\ell)$ be a function such that $|F(k,\ell)| = O\left((1+\log(k\ell))^2\right)$ for $k,\ell \ge 1$. We have, for large N,

$$\sum_{1\le k<N_3}\sum_{\ell\ge 1}\int_0^1\int_0^1\int_0^1 F(k,\ell)\,h_{N,m}(\lambda,\lambda',k)\,q_{N,m,k,\ell}(\lambda,\lambda',z)\,dz\,d\lambda'\,d\lambda$$
$$= \sum_{1\le k<N_3}\sum_{\ell\ge 1}\int_0^{a(m,N)}\int_{b(m,N)}^{a(m,N)}\int_{N^{-3/8}}^1 F(k,\ell)\,h_{N,m}(\lambda,\lambda',k)\,q_{N,m,k,\ell}(\lambda,\lambda',z)\,dz\,d\lambda'\,d\lambda$$
$$+O(N^{-1/16}(\log\,N)^2) \ .$$

Lemma 33 Let $N_1 \le m < N_2$, $1 \le k < N_3$, and $(\lambda, \lambda', z) \in (0, a(m,N)) \times (b(m,N),\ a(m,N)) \times (N^{-3/8},\ 1)$. Then, for large N,

$$\sum_{\ell \ge 1} H_\ell\, q_{N,m,k,\ell}(\lambda, \lambda', z) = \left(\ln(N\lambda' z) + \gamma + O(N^{-1/200})\right) k(1-z)^{k-1} \ .$$

Lemma 34 For all $1 \le k < N_3$, we have, for large N,

$$\begin{aligned} \int_{N^{-3/8}}^{1} k(1-z)^{k-1} \ln z \, dz &= -H_k + O\left(N^{-3/8}(\log N)\right) \ , \text{ and} \\ \int_{N^{-3/8}}^{1} k(1-z)^{k-1} \, dz &= 1 - O(N^{-1/16}) \ . \end{aligned}$$

5.3 Formulas involving $\psi_{j,h}$

Lemma 35 (a) For $j \in \{0,1\}$ and each $k \ge 1$, the integral $\beta_{j,k} = \int_0^\infty \int_0^\infty \int_0^\infty \psi_{j,k}(x,u,v)\, dx\, dv\, du$ exists and is finite.

(b) Let $j \in \{0,1\}$, and $F(k)$ be a nonnegative real-valued function on integers $k \ge 0$. Suppose $B, D > 2$, , and $X_2 > 1 > X_1 \ge 0$. Then

$$\begin{aligned} &\left| \sum_{1 \le k \le D} F(k) \int_0^B \int_0^B \int_{X_1}^{X_2} \psi_{j,k}(x,u,v)\, dx\, dv\, du - \sum_{1 \le k \le D} F(k)\, \beta_{j,k} \right| \\ &\qquad = O\Big(\frac{C(D)(\log B)^j}{B} + e^{-X_2} C(D) + \sqrt{X_1}\, C(D) \Big) \ , \end{aligned}$$

where $C(D) = \max\{F(k) \mid 1 \le k \le D\}$.

(c) Let $j \in \{0,1\}$. For all $k \ge 200$, $\beta_{j,k} = O\Big(\frac{(\log k)^j}{k^{3/2}}\Big)$.

Definition 13 For any sequence $(a_1, a_2, \ldots, a_k, \ldots)$ of real numbers, write $<< a_k >>$ for $\sum_{k \ge 1} a_k \beta_{0,k}$ if the sum exists; write $((a_k))$ for $\sum_{k \ge 1} a_k\, \beta_{1,k}$ if the sum exists.

Lemma 36

$$\begin{aligned} << H_k >> &= \sqrt{\pi} \ , \\ << H_k^{(2)} >> &= \frac{\sqrt{\pi}}{2} \sum_{m \ge 1} \frac{4^m((m-1)!)^2}{(2m+1)!} \ , \\ -2((H_k)) + << H_k^2 >> &= \gamma << H_k >> + \sqrt{\pi} \sum_{m \ge 1} \frac{1}{m(2m+1)^2} \ . \end{aligned}$$

6 Evaluation Step One

Definition 14 For $N \geq 2$, let

$$T_N = \sum_{1 \leq m \leq N/2} \sum_{1 \leq k \leq N-2m} p_{N,m}\Big(H_k^2 + H_k - H_k^{(2)} - H_k\, H_{N-m}\Big) \times \int_0^1 \int_0^1 h_{N,m}(\lambda, \lambda', k)\, d\lambda\, d\lambda' \ ,$$

and

$$W_N = \sum_{1 \leq m \leq N/2} \sum_{1 \leq k \leq N-2m} \sum_{\ell \geq 1} p_{N,m}\, H_k\, H_\ell \int_0^1 \int_0^1 \int_0^1 h_{N,m}(\lambda, \lambda', k)\, q_{N,m,k,\ell}(\lambda, \lambda', k)\, d\lambda\, d\lambda'\, dz \ .$$

From Theorems 1, 2 and the fact that $p_{N,m} = 0$ when $2m > N$, we obtain, for $n \geq 2$,

$$Var(B_n) = 2 \sum_{1 < N \leq n} (T_N + 2W_N) + O(n \log n) \ . \tag{46}$$

We will, in this and the next two sections, derive the asymptotic form for T_N, W_N as $N \to \infty$, and then use (43) to prove Theorem 3. As a first step, we will prove the next lemmma in this section.

Lemma 37 For large N,

$$T_N = \sum_{N_1 \leq m < N_2} \sum_{1 \leq k < N_3} e^{-m^2/N}\Big(H_k^2 - H_k^{(2)} - H_k(\ln N + \gamma - 1)\Big) \times \int_0^1 \int_0^1 \hat{h}_{N,m}(\lambda, \lambda', k)\, d\lambda\, d\lambda' + O(N^{7/16}(\log N)^2) \ .$$

Proof. From Lemma 26 we have

$$\begin{aligned}
&\sum_{1 \leq m < N_1} \sum_{1 \leq k \leq N-2m} p_{N,m}\Big(H_k^2 + H_k - H_k^{(2)} - H_k\, H_{N-m}\Big) \times \int_0^1 \int_0^1 h_{N,m}(\lambda, \lambda', k)\, d\lambda\, d\lambda' \\
&= \sum_{1 \leq m < N_1} O((\log N)^2) \\
&= O(N_1 (\log N)^2) \ .
\end{aligned} \tag{47}$$

Also, from Lemma 24 and Lemma 26, we have

$$\begin{aligned}
&\sum_{N_2 \leq m \leq N/2} \sum_{1 \leq k \leq N-2m} p_{N,m}\Big(H_k^2 + H_k - H_k^{(2)} - H_k\, H_{N-m}\Big) \times \int_0^1 \int_0^1 h_{N,m}(\lambda, \lambda', k)\, d\lambda\, d\lambda' \\
&= \sum_{N_2 \leq m \leq N/2} O\Big(e^{-N^{2\epsilon}}\, (\log N)^2\Big) \\
&= O\Big(N (\log N)^2\, e^{-N^{2\epsilon}}\Big) \ .
\end{aligned} \tag{48}$$

It follows from (47), (48) that

$$\begin{aligned} T_N &= \sum_{N_1 \le m < N_2} \sum_{1 \le k \le N-2m} p_{N,m}\Big(H_k^2 + H_k - H_k^{(2)} - H_k H_{N-m}\Big) \\ &\qquad \times \int_0^1 \int_0^1 h_{N,m}(\lambda, \lambda', k)\, d\lambda\, d\lambda' \\ &\quad + O\Big(N_1 (\log N)^2 + N (\log N)^2 e^{-N^{2\epsilon}}\Big) . \end{aligned} \tag{49}$$

Using Lemma 24 and Lemma 29, we obtain from (49)

$$\begin{aligned} T_N &= \sum_{N_1 \le m < N_2} \sum_{1 \le k < N_3} p_{N,m}\Big(H_k^2 + H_k - H_k^{(2)} - H_k H_{N-m}\Big) \\ &\qquad \times \int_0^1 \int_0^1 h_{N,m}(\lambda, \lambda', k)\, d\lambda\, d\lambda' \\ &\quad + \sum_{N_1 \le m < N_2} \sum_{N_3 \le k \le N-2m} O((\log N)^2) \int_0^1 \int_0^1 h_{N,m}(\lambda, \lambda', k)\, d\lambda\, d\lambda' \\ &\quad + O(N_1 (\log N)^2) \\ &= \sum_{N_1 \le m < N_2} \sum_{1 \le k < N_3} \Big(1 + O(N^{-1/2+3\epsilon})\Big) e^{-m^2/N} \int_0^1 \int_0^1 h_{N,m}(\lambda, \lambda', k)\, d\lambda\, d\lambda' \\ &\qquad \times \left(H_k^2 + H_k - H_k^{(2)} - H_k \left(\ln(N-m) + \gamma + O\Big(\frac{1}{(N-m)}\Big)\right)\right) \\ &\quad + O\Big(\frac{N^2 (\log N)^2}{N^9}\Big) + O(N_1 (\log N)^2) \\ &= \sum_{N_1 \le m < N_2} \sum_{1 \le k < N_3} e^{-m^2/N} \int_0^1 \int_0^1 h_{N,m}(\lambda, \lambda', k)\, d\lambda\, d\lambda' \\ &\qquad \times \left(H_k^2 - H_k^{(2)} - H_k\Big(\ln N + \gamma - 1 + O(\frac{m}{N})\Big)\right) \\ &\quad + O(N^{-1/2+3\epsilon}) \sum_{N_1 \le m < N_2} \sum_{1 \le k < N_3} e^{-m^2/N} (\log N)^2 \\ &\qquad \times \int_0^1 \int_0^1 h_{N,m}(\lambda, \lambda', k)\, d\lambda\, d\lambda' \\ &\quad + O(N_1 (\log N)^2) . \end{aligned}$$

Applying Lemmas 25 and 26, we have then

$$\begin{aligned} T_N &= \sum_{N_1 \le m < N_2} \sum_{1 \le k < N_3} e^{-m^2/N} \big(H_k^2 - H_k^{(2)} - H_k\big(\ln N + \gamma - 1\big)\big) \\ &\qquad \times \int_0^1 \int_0^1 h_{N,m}(\lambda, \lambda', k)\, d\lambda\, d\lambda' \\ &\quad + O\Big((N_2/N + N^{-1/2+3\epsilon}) \cdot (\log N)^2\Big) \\ &\qquad \times \sum_{N_1 \le m < N_2} e^{-m^2/N} + O(N_1 (\log N)^2) \end{aligned}$$

$$
\begin{aligned}
&= \sum_{N_1 \le m < N_2} \sum_{1 \le k < N_3} e^{-m^2/N} \Big(H_k^2 - H_k^{(2)} - H_k(\ln N + \gamma - 1) \Big) \\
&\qquad \times \int_0^1 \int_0^1 h_{N,m}(\lambda, \lambda', k) \, d\lambda \, d\lambda' \\
&\quad + O(N_1 (\log N)^2) \ .
\end{aligned} \tag{50}
$$

From (50) and Lemmas 25-28, we obtain

$$
\begin{aligned}
T_N &= \sum_{N_1 \le m < N_2} \sum_{1 \le k < N_3} e^{-m^2/N} \Big(H_k^2 - H_k^{(2)} - H_k(\ln N + \gamma - 1) \Big) \\
&\qquad \times \int_0^{a(m,N)} \int_0^{a(m,N)} h_{N,m}(\lambda, \lambda', k) \, d\lambda \, d\lambda' \\
&\quad + O\Big(N^2 (\log N)^2 \frac{1}{N^9} \Big) + O(N_1 (\log N)^2) \\
&= \sum_{N_1 \le m < N_2} \sum_{1 \le k < N_3} e^{-m^2/N} \Big(H_k^2 - H_k^{(2)} - H_k(\ln N + \gamma - 1) \Big) \\
&\qquad \times \int_0^{a(m,N)} \int_0^{a(m,N)} \hat{h}_{N,m}(\lambda, \lambda', k) \, d\lambda \, d\lambda' \\
&\quad + O(N^{-1/8}) \sum_{N_1 \le m < N_2} e^{-m^2/N} (\log N)^2 \\
&\qquad \times \sum_{k \ge 0} \int_0^1 \int_0^1 \hat{h}_{N,m}(\lambda, \lambda', k) \, d\lambda \, d\lambda' \\
&\quad + O(N_1 (\log N)^2) \\
&= \sum_{N_1 \le m < N_2} \sum_{1 \le k < N_3} e^{-m^2/N} \Big(H_k^2 - H_k^{(2)} - H_k(\ln N + \gamma - 1) \Big) \\
&\qquad \times \int_0^1 \int_0^1 \hat{h}_{N,m}(\lambda, \lambda', k) \, d\lambda \, d\lambda' \\
&\quad + O\Big(N^2 (\log N)^2 \frac{1}{N^9} \Big) \\
&\quad + O(N^{-1/8}) \cdot O\Big(\sqrt{N} \, (\log N)^2 \Big) \\
&\quad + O(N_1 (\log N)^2) \ .
\end{aligned}
$$

This proves Lemma 37. □

7 Evaluation Step Two

We will prove the following lemma (recall that $\kappa = 1/200$):

Lemma 38 For large N,

$$\begin{aligned} W_N &= \sum_{N_1 \le m < N_2} \sum_{1 \le k < N_3} e^{-m^2/N} H_k \\ &\qquad \times \int_0^1 \int_0^1 \hat{h}_{N,m}(\lambda, \lambda', k)(\ln(N\lambda') + \gamma - H_k)\, d\lambda'\, d\lambda \\ &\quad + O\Big(N^{1/2-\kappa} \log N \Big) . \end{aligned}$$

Proof. Let

$$\begin{aligned} G_1 &= \sum_{N_1 \le m < N_2} \sum_{1 \le k < N_3} \sum_{\ell \ge 1} p_{N,m} H_k H_\ell \\ &\qquad \times \int_0^1 \int_0^1 \int_0^1 h_{N,m}(\lambda, \lambda', k)\, q_{N,m,k,\ell}(\lambda, \lambda', z) dz\, d\lambda'\, d\lambda , \\ G_2 &= \sum_{N_1 \le m < N_2} \sum_{1 \le k < N_3} \sum_{\ell \ge 1} p_{N,m} H_k H_\ell \\ &\qquad \times \int_0^{a(m,N)} \int_{b(m,N)}^{a(m,N)} \int_{N^{-3/8}}^1 h_{N,m}(\lambda, \lambda', k)\, q_{N,m,k,\ell}(\lambda, \lambda', z) dz\, d\lambda'\, d\lambda , \\ G_3 &= \sum_{N_1 \le m < N_2} \sum_{1 \le k < N_3} \sum_{\ell \ge 1} e^{-m^2/N} H_k H_\ell \\ &\qquad \times \int_0^{a(m,N)} \int_{b(m,N)}^{a(m,N)} \int_{N^{-3/8}}^1 \hat{h}_{N,m}(\lambda, \lambda', k)\, q_{N,m,k,\ell}(\lambda, \lambda', z) dz\, d\lambda'\, d\lambda \end{aligned}$$

Using Lemmas 24, 31, we obtain

$$\begin{aligned} |W_N - G_1| &\le \sum_{1 \le m < N_1} O\Big(e^{-m^2/N} (\log N)^2\Big) \sum_{k \ge 1} \sum_{\ell \ge 1} \\ &\qquad \int_0^1 \int_0^1 \int_0^1 h_{N,m}(\lambda, \lambda', k) q_{N,m,k,\ell}(\lambda, \lambda', z)\, dz\, d\lambda', d\lambda \\ &\quad + \sum_{N_2 \le m \le N/2} O\Big(e^{-n^{2\epsilon}} (\log N)^2\Big) \sum_{k \ge 1} \sum_{\ell \ge 1} \\ &\qquad \int_0^1 \int_0^1 \int_0^1 h_{N,m}(\lambda, \lambda', k) q_{N,m,k,\ell}(\lambda, \lambda', z)\, dz\, d\lambda', d\lambda \\ &\quad + O((\log N)^2) \cdot \sum_{N_1 \le m < N_2} \sum_{N_3 \le k \le N-2m} \sum_{\ell \ge 1} \\ &\qquad \int_0^1 \int_0^1 \int_0^1 h_{N,m}(\lambda, \lambda', k) q_{N,m,k,\ell}(\lambda, \lambda', z)\, dz\, d\lambda', d\lambda \\ &= O((\log N)^2) \Bigg\{ \sum_{1 \le m < N_1} e^{-m^2/N} \sum_{k \ge 1} \int_0^1 \int_0^1 h_{N,m}(\lambda, \lambda', k)\, d\lambda'\, d\lambda \end{aligned}$$

$$
\begin{aligned}
&+ e^{-N^{2\epsilon}} \sum_{N_2 \le m \le N/2} \sum_{k\ge 1} \int_0^1 \int_0^1 h_{N,m}(\lambda,\lambda',k)\, d\lambda'\, d\lambda \\
&+ \sum_{N_1 \le m < N_2} \sum_{N_3 \le k \le N-2m} \int_0^1 \int_0^1 h_{N,m}(\lambda,\lambda',k)\, d\lambda'\, d\lambda \Bigg\} .
\end{aligned}
$$

Now, from Lemmas 26, 29, we have

$$
\begin{aligned}
|W_N - G_1| &= O((\log N)^2) \left\{ \sum_{1\le m<N_1} e^{-m^2/N} + N\, e^{-N^{2\epsilon}} + O\Big(\frac{1}{N^8}\Big) \right\} \\
&= O\Big(N_1 (\log N)^2\Big) . \qquad (51)
\end{aligned}
$$

Using Lemmas 24, 25 and 32, we obtain

$$
\begin{aligned}
|G_1 - G_2| \le & \sum_{N_1 \le m < N_2} O(e^{-m^2/N}) \sum_{1\le k<N_3} \sum_{\ell\ge 1} \\
& \Big| \int_0^1 \int_0^1 \int_0^1 H_k H_\ell\, h_{N,m}(\lambda,\lambda',k) q_{N,m,k,\ell}(\lambda,\lambda',z)\, dz\, d\lambda'\, d\lambda \\
& - \int_0^{a(m,N)} \int_{b(m,N)}^{a(m,N)} \int_{N^{-3/8}}^1 H_k H_\ell\, h_{N,m}(\lambda,\lambda',k) q_{N,m,k,\ell}(\lambda,\lambda',z)\, dz\, d\lambda', d\lambda \Big| \\
= & O\Big((\log N)^2\, N^{-1/16} \sum_{N_1\le m<N_2} e^{-m^2/N}\Big) \\
= & O((\log N)^2\, N^{7/16}) . \qquad (52)
\end{aligned}
$$

Similarly, we have from Lemmas 24, 27, and 31

$$
\begin{aligned}
|G_2 - G_3| \le & \sum_{N_1 \le m < N_2} \sum_{1\le k<N_3} \sum_{\ell\ge 1} |\, p_{N,m} - e^{-m^2/N}\,|\; H_k\, H_\ell \\
& \times \int_0^{a(m,N)} \int_{b(m,N)}^{a(m,N)} \int_{N^{-3/8}}^1 h_{N,m}(\lambda,\lambda',k)\; q_{N,m,k,\ell}(\lambda,\lambda',z) dz\, d\lambda'\, d\lambda \\
& + \sum_{N_1 \le m < N_2} \sum_{1\le k<N_3} \sum_{\ell\ge 1} e^{-m^2/N} H_k\, H_\ell \int_0^{a(m,N)} \int_{b(m,N)}^{a(m,N)} \int_{N^{-3/8}}^1 \\
& \times |\, h_{N,m}(\lambda,\lambda',k) - \hat{h}_{N,m}(\lambda,\lambda',k)\,|\; q_{N,m,k,\ell}(\lambda,\lambda',z) dz\, d\lambda'\, d\lambda \\
= & O(N^{-1/2+3\epsilon}) \sum_{N_1 \le m < N_2} \sum_{1\le k<N_3} \sum_{\ell\ge 1} O((\log N)^2)\, e^{-m^2/N} \\
& \times \int_0^1 \int_0^1 \int_0^1 h_{N,m}(\lambda,\lambda',k) q_{N,m,k,\ell}(\lambda,\lambda',z)\, dz\, d\lambda'\, d\lambda \\
& + O(N^{-1/8}) \sum_{N_1 \le m < N_2} \sum_{1\le k<N_3} \sum_{\ell\ge 1} O((\log N)^2)\, e^{-m^2/N} \\
& \times \int_0^1 \int_0^1 \int_0^1 \hat{h}_{N,m}(\lambda,\lambda',k) q_{N,m,k,\ell}(\lambda,\lambda',z)\, dz\, d\lambda'\, d\lambda
\end{aligned}
$$

$$= O(N^{-1/2+3\epsilon}(\log N)^2) \sum_{N_1 \le m < N_2} \sum_{1 \le k < N_3} e^{-m^2/N} \int_0^1 \int_0^1 h_{N,m}(\lambda, \lambda', k)\, d\lambda'\, d\lambda \ .$$

$$+ O(N^{-1/8}(\log N)^2) \sum_{N_1 \le m < N_2} \sum_{1 \le k < N_3} e^{-m^2/N} \int_0^1 \int_0^1 \hat{h}_{N,m}(\lambda, \lambda', k)\, d\lambda'\, d\lambda \ .$$

Using Lemmas 25 and 26, we obtain

$$|G_2 - G_3| = O(N^{3/8}(\log N)^2) \ . \tag{53}$$

We now evaluate G_3. Let $N_1 \le m < N_2$, $1 \le k < N_3$, and $(\lambda, \lambda', z) \in \Big(0,\ a(m,N)\Big) \times \Big(b(m,N),\ a(m,N)\Big) \times (N^{-3/8}, 1)$. By Lemma 33,

$$\sum_{\ell \ge 0} H_\ell\, q_{N,m,k,\ell}(\lambda, \lambda', z) = \Big(\ln(N\lambda' z) + \gamma + O(N^{-1/200})\Big)\, k(1-z)^{k-1} \ .$$

This implies that

$$\int_{N^{-3/8}}^1 \sum_{\ell \ge 0} H_\ell\, q_{N,m,k,\ell}(\lambda, \lambda', z)\, dz = \Big(\ln(N\lambda') + \gamma + O(N^{-1/200})\Big)$$
$$\times \int_{N^{-3/8}}^1 k(1-z)^{k-1}\, dz + \int_{N^{-3/8}}^1 k(1-z)^{k-1} \ln z\, dz \ .$$

Using Lemma 34, we get

$$\begin{aligned} \int_{N^{-3/8}}^1 \sum_{\ell \ge 0} & H_\ell\, q_{N,m,k,\ell}(\lambda, \lambda', z)\, dz \\ &= \Big(\ln(N\lambda') + \gamma + O(N^{-1/200})\Big)(1 - O(N^{-1/16})) \\ &\qquad - H_k + O(N^{-3/8}(\log N)) \\ &= \ln(N\lambda') + \gamma - H_k + O(N^{-1/200}) \ . \end{aligned} \tag{54}$$

From (54), we have

$$\begin{aligned} G_3 \ = \ & \sum_{N_1 \le m < N_2} \sum_{1 \le k < N_3} e^{-m^2/N} H_k \\ & \qquad \times \int_0^{a(m,N)} \int_{b(m,N)}^{a(m,N)} (\ln(N\lambda') + \gamma - H_k)\, \hat{h}_{N,m}(\lambda, \lambda', k)\, d\lambda'\, d\lambda \\ + \ & O(N^{-1/200}) \sum_{N_1 \le m < N_2} \sum_{1 \le k < N_3} e^{-m^2/N} H_k \\ & \qquad \times \int_0^{a(m,N)} \int_{b(m,N)}^{a(m,N)} \hat{h}_{N,m}(\lambda, \lambda', k)\, d\lambda'\, d\lambda \ . \end{aligned}$$

Using Lemma 30, we obtain

$$G_3 \ = \ \sum_{N_1 \le m < N_2} \sum_{1 \le k < N_3} e^{-m^2/N} H_k$$

$$
\begin{aligned}
& \times \int_0^1 \int_0^1 (\ln(N\lambda') + \gamma - H_k)\, \hat{h}_{N,m}(\lambda, \lambda', k)\, d\lambda'\, d\lambda \\
+ & \sum_{N_1 \le m \le N_2} e^{-m^2/N}\, O(N^{-1/10}(\log N)^4) \\
+ & \ O(N^{-1/200}) \sum_{N_1 \le m \le N_2} e^{-m^2/N}\, (\log N) \\
& \times \sum_{k \ge 1} \int_0^1 \int_0^1 \hat{h}_{N,m}(\lambda, \lambda', k)\, d\lambda'\, d\lambda \ .
\end{aligned}
$$

Now using Lemmas 25 and 26, we get

$$
\begin{aligned}
G_3 \ = \ & \sum_{N_1 \le m < N_2} \sum_{1 \le k < N_3} e^{-m^2/N}\, H_k \int_0^1 \int_0^1 \hat{h}_{N,m}(\lambda, \lambda', k)\, (\ln(N\lambda') + \gamma - H_k)\, d\lambda'\, d\lambda \\
& + O(N^{1/2-\kappa} \log N) \ . \qquad (55)
\end{aligned}
$$

Lemma 38 follows from (51), (52), (53) and (55).

8 Evaluation Step Three

We finish the proof of Theorem 3 in this section. From Lemma 37 and 38, we obtain

$$\begin{aligned}
T_N + 2W_N &= \sum_{N_1 \le m < N_2} \sum_{1 \le k < N_3} e^{-m^2/N} \\
&\qquad \times \int_0^1 \int_0^1 \Big(2H_k \ln(\sqrt{N}\,\lambda') + (\gamma+1)\,H_k - H_k^2 - H_k^{(2)}\Big) \\
&\qquad \times \hat{h}_{N,m}(\lambda,\lambda',k)\,d\lambda'\,d\lambda + O(N^{1/2-\kappa}\log N) \\
&= 2 \sum_{1 \le k < N_3} H_k \int_0^1 \int_0^1 \sum_{N_1 \le m < N_2} e^{-m^2/N} \\
&\qquad \times \hat{h}_{N,m}(\lambda,\lambda',k) \ln(\sqrt{N}\,\lambda')\,d\lambda'\,d\lambda \\
&+ \sum_{1 \le k < N_3} \Big((\gamma+1)\,H_k - H_k^2 - H_k^{(2)}\Big) \int_0^1 \int_0^1 \sum_{N_1 \le m < N_2} e^{-m^2/N} \\
&\qquad \times \hat{h}_{N,m}(\lambda,\lambda',k)\,d\lambda'\,d\lambda \\
&+ O(N^{1/2-\kappa}\log N) \;. \qquad (56)
\end{aligned}$$

Let $g_{N,k,\lambda,\lambda'}(s)$ be defined as follows: for $s \ge 0$,

$$g_{N,k,\lambda,\lambda'}(s) = \frac{(\lambda\lambda' N)^k}{k!}\, e^{-\lambda\lambda' N}\, s^2\, e^{-(\lambda+\lambda')s - s^2/N}.$$

Then, for integers $m \ge 0$, $g_{N,k,\lambda,\lambda'}(m) = e^{-m^2/N}\,\hat{h}_{N,m}(\lambda,\lambda',k)$. Write $N_i' = \lceil N_i \rceil$ for $i = 1,2$. By Euler's Summation Formula (see, e.g. Knuth [K2, Section 1.2.11.2]), we have

$$\begin{aligned}
\sum_{N_1 \le m < N_2} g_{N,k,\lambda,\lambda'}(m) &= \int_{N_1'}^{N_2'} g_{N,k,\lambda,\lambda'}(s)\,ds - \frac{1}{2}\Big(g_{N,k,\lambda,\lambda'}(N_2') - g_{N,k,\lambda,\lambda'}(N_1')\Big) \\
&\quad + \int_{N_1'}^{N_2'} B_1(s - \lfloor s \rfloor)\, g'_{N,k,\lambda,\lambda'}(s)\,ds \;, \qquad (57)
\end{aligned}$$

where $B_1(x) = x - 1/2$ is the Bernoulli polynomial of degree 1.

For $1 \le k < N_3$, $0 < \lambda, \lambda' < 1$, $N_1' \le s < N_2'$, it is easy to see that

$$\left|g_{N,k,\lambda,\lambda'}(N_2')\right| \le \frac{(\lambda\lambda' N)^k}{k!}\, e^{-\lambda\lambda' N}\, N^{1+2\epsilon}\, e^{-N^{2\epsilon}} \;, \qquad (58)$$

$$\left|g_{N,k,\lambda,\lambda'}(N_1')\right| \le \frac{(\lambda\lambda' N)^k}{k!}\, e^{-\lambda\lambda' N}\, N^{7/8}\, e^{-(\lambda+\lambda')N^{7/16}} \;, \qquad (59)$$

and

$$\begin{aligned}
\left|g'_{N,k,\lambda,\lambda'}(s)\right| &= \left|-\frac{2s}{N} - (\lambda+\lambda') + \frac{2}{s}\right| g_{N,k,\lambda,\lambda'}(s) \\
&= \Big(\lambda + \lambda' + O(N^{-7/16})\Big)\, g_{N,k,\lambda,\lambda'}(s) \;. \qquad (60)
\end{aligned}$$

Lemma 39

$$\sum_{1\le k<N_3}\left((\gamma+1)\,H_k - H_k^2 - H_k^{(2)}\right)\int_0^1\int_0^1 \sum_{N_1\le m<N_2} e^{-m^2/N}\,\hat{h}_{N,m}(\lambda,\lambda',k)\,d\lambda'\,d\lambda$$
$$= \sqrt{N}\{(\gamma+1) << H_k >> - << H_k^2 >> - << H_k^{(2)} >>\} + O(N^{15/32}(\log N)^2).$$

Proof. From (57) - (60), we obtain

$$\sum_{1\le k<N_3}\left((\gamma+1)\,H_k - H_k^2 - H_k^{(2)}\right)\int_0^1\int_0^1 \sum_{N_1\le m<N_2} e^{-m^2/N}\,\hat{h}_{N,m}(\lambda,\lambda',k)\,d\lambda'\,d\lambda$$
$$= \sum_{1\le k<N_3}\left((\gamma+1)\,H_k - H_k^2 - H_k^{(2)}\right)\int_0^1\int_0^1\int_{N_1'}^{N_2'} g_{N,k,\lambda,\lambda'}(s)\,ds\,d\lambda'\,d\lambda + L_1\,, \quad (61)$$

where

$$\begin{aligned}
|L_1| \;\le\; & \frac{1}{2}\int_0^1\int_0^1 \sum_{1\le k<N_3}\left|(\gamma+1)\,H_k - H_k^2 - H_k^{(2)}\right| \\
& \times \frac{(\lambda\lambda' N)^k}{k!}\,e^{-\lambda\lambda' N}\,N^{1+2\epsilon}\,e^{-N^{2\epsilon}}\,d\lambda'\,d\lambda \\
+\; & \frac{1}{2}\int_0^1\int_0^1 \sum_{1\le k<N_3}\left|(\gamma+1)\,H_k - H_k^2 - H_k^{(2)}\right| \\
& \times \frac{(\lambda\lambda' N)^k}{k!}\,e^{-\lambda\lambda' N}\,N^{7/8}\,e^{-(\lambda+\lambda')N^{7/16}}\,d\lambda'\,d\lambda \\
+\; & \sum_{1\le k<N_3}\int_0^1\int_0^1\int_{N_1'}^{N_2'}\left|(\gamma+1)\,H_k - H_k^2 - H_k^{(2)}\right| \\
& \times\left(\lambda+\lambda'+O(N^{-7/16})\right)g_{N,k,\lambda,\lambda'}(s)\,ds\,d\lambda'\,d\lambda\;.
\end{aligned}$$

Clearly,

$$\begin{aligned}
L_1 \;=\; & O((\log N)^2)\,N^{1+2\epsilon}\,e^{-N^{2\epsilon}} + O((\log N)^2\,N^{7/8})\left(\int_0^1 e^{-\lambda N^{7/16}}\,d\lambda\right)^2 \\
& + O\left((\log N)^2\right)\int_0^1\int_0^1\int_{N_1'}^{N_2'}\left(\lambda+\lambda'+O(N^{-7/16})\right)s^2 \\
& \times e^{-s^2/N-(\lambda+\lambda')s}\,ds\,d\lambda'\,d\lambda \\
=\; & O((\log N)^2\,N^{1+2\epsilon}\,e^{-N^{2\epsilon}}) \\
& + O((\log N)^2\,N^{7/8})\cdot O\left((N^{-7/16}\int_0^\infty e^{-x}\,dx)^2\right) \\
& + O((\log N)^2)\left\{2\int_{N_1'}^{N_2'} s^2 e^{-s^2/N}\right. \\
& \times\left(\int_0^1 \lambda\,e^{-\lambda s}\,d\lambda\right)\left(\int_0^1 e^{-\lambda' s}\,d\lambda'\right)ds
\end{aligned}$$

$$+ O(N^{-7/16}) \int_{N_1}^{N_2} s^2\, e^{-s^2/N} \Big(\int_0^1 e^{-\lambda s} \Big)^2 ds \Big\}$$

$$\begin{aligned}
&= O((\log N)^2) + O((\log N)^2) \\
&\qquad \times \Big\{ \int_{N_1'}^{N_2'} \frac{1}{s}\, ds + O(N^{-7/16}) \int_0^\infty e^{-s^2/N}\, ds \Big\} \\
&= O((\log N)^2) \Big\{ \log N + O(N^{-7/16} N^{1/2}) \Big\} \\
&= O(N^{1/16} (\log N)^2)\ . \qquad (62)
\end{aligned}$$

Let $x_1 = N_1'/\sqrt{N}$ and $x_2 = N_2'/\sqrt{N}$. From (61) and (62), we obtain

$$\begin{aligned}
&\sum_{1 \le k < N_3} \Big((\gamma+1)\, H_k - H_k^2 - H_k^{(2)} \Big) \int_0^1 \int_0^1 \sum_{N_1 \le m < N_2} e^{-m^2/N}\, \hat{h}_{N,m}(\lambda, \lambda', k)\, d\lambda'\, d\lambda \\
&= \sum_{1 \le k < N_3} \Big((\gamma+1)\, H_k - H_k^2 - H_k^{(2)} \Big) \int_0^1 \int_0^1 \int_{N_1'}^{N_2'} \\
&\qquad \frac{(\lambda\lambda' N)^k}{k!}\, e^{-\lambda\lambda' N}\, s^2\, e^{-(\lambda+\lambda')s - s^2/N}\, ds\, d\lambda'\, d\lambda \\
&\quad + O(N^{1/16} (\log N)^2) \\
&= \sum_{1 \le k < N_3} \frac{\Big((\gamma+1)\, H_k - H_k^2 - H_k^{(2)} \Big)}{k!} \int_0^{\sqrt{N}} \int_0^{\sqrt{N}} \int_{x_1}^{x_2} \\
&\qquad (uv)^k\, e^{-uv}\, N\, x^2\, e^{-(u+v)x - x^2}\, \frac{1}{\sqrt{N}}\, dx\, dv\, du \\
&\quad + O(N^{1/8} (\log N)^2) \\
&= \sqrt{N} \Bigg(\sum_{1 \le k < N_3} (\gamma+1) H_k \int_0^{\sqrt{N}} \int_0^{\sqrt{N}} \int_{x_1}^{x_2} \psi_{0,k}(x,u,v)\, dx\, dv\, du \\
&\qquad - \sum_{1 \le k < N_3} H_k^2 \int_0^{\sqrt{N}} \int_0^{\sqrt{N}} \int_{x_1}^{x_2} \psi_{0,k}(x,u,v)\, dx\, dv\, du \\
&\qquad - \sum_{1 \le k < N_3} H_k^{(2)} \int_0^{\sqrt{N}} \int_0^{\sqrt{N}} \int_{x_1}^{x_2} \psi_{0,k}(x,u,v)\, dx\, dv\, du \Bigg) \\
&\quad + O(N^{1/8} (\log N)^2)\ .
\end{aligned}$$

Using Lemma 35, we then obtain

$$\begin{aligned}
&\sum_{1 \le k < N_3} \Big((\gamma+1)\, H_k - H_k^2 - H_k^{(2)} \Big) \int_0^1 \int_0^1 \sum_{N_1 \le m < N_2} e^{-m^2/N}\, \hat{h}_{N,m}(\lambda, \lambda', k)\, d\lambda'\, d\lambda \\
&= \sqrt{N} \Bigg\{ \sum_{1 \le k < N_3} \Big((\gamma+1)\, H_k - H_k^2 - H_k^{(2)} \Big)\, \beta_{0,k} + (\log N)^2 \cdot O\Big(\frac{1}{\sqrt{N}} + e^{-x_2} + \sqrt{x_1} \Big) \Bigg\}
\end{aligned}$$

$$
\begin{aligned}
&+ O(N^{1/8}(\log N)^2) \\
&= \sqrt{N}\left\{(\gamma+1) << H_k >> - << H_k^2 >> - << H_k^{(2)} >> + O\Big(\frac{(\log N)^2}{\sqrt{N_3}}\Big)\right\} \\
&\quad + O\Big(N^{15/32}(\log N)^2\Big) \ .
\end{aligned}
$$

This proves Lemma 39. □

Lemma 40

$$
\sum_{1\le k<N_3} H_k \int_0^1\int_0^1 \sum_{N_1\le m<N_2} e^{-m^2/N}\,\hat{h}_{N,m}(\lambda,\lambda',k)\ln(\sqrt{N}\,\lambda')\ d\lambda'\,d\lambda
$$
$$
= \sqrt{N}\,((H_k)) + O(N^{15/32}(\log N)^2)\ .
$$

Proof. We follow the same approach as used in the proof of the preceding lemma. Again, let $x_1 = N_1'/\sqrt{N}$ and $x_2 = N_2'/\sqrt{N}$. From (57) - (60), we obtain

$$
\begin{aligned}
&\sum_{1\le k<N_3} H_k \int_0^1\int_0^1 \sum_{N_1\le m<N_2} e^{-m^2/N}\,\hat{h}_{N,m}(\lambda,\lambda',k)\ln(\sqrt{N}\,\lambda')\ d\lambda'\,d\lambda \\
&\quad = \sum_{1\le k<N_3} H_k \int_0^1\int_0^1\int_{N_1'}^{N_2'} g_{N,k,\lambda,\lambda'}(s)\ln(\sqrt{N}\,\lambda')\,ds\,d\lambda'\,d\lambda + L_2\ ,
\end{aligned}
\tag{63}
$$

where

$$
\begin{aligned}
|L_2| &\le \frac{1}{2}\int_0^1\int_0^1 O((\log N))\,N^{1+2\epsilon}\,e^{-N^{2\epsilon}}\ \ln(\sqrt{N}\,\lambda')\,d\lambda'\,d\lambda \\
&\quad + \frac{1}{2}\int_0^1\int_0^1 O(\log N)\,N^{7/8}\,e^{-(\lambda+\lambda')N^{7/16}}\ \ln(\sqrt{N}\,\lambda')\,d\lambda'\,d\lambda \\
&\quad + O(\log N)\int_0^1\int_0^1\int_{N_1'}^{N_2'}\Big(\lambda+\lambda'+O(N^{-7/16})\Big)\,s^2 \\
&\qquad\qquad \times e^{-s^2/N-(\lambda+\lambda')s}\ \ln(\sqrt{N}\,\lambda')\,ds\,d\lambda'\,d\lambda \\
&= O\Big(e^{-N^{2\epsilon}}\,N^{1+2\epsilon}(\log N)^2\Big) \\
&\quad + O\Big((\log N)\,N^{7/8}\Big)\left|\int_0^1 e^{-\lambda N^{7/16}}\,d\lambda\right|\cdot\left|\int_0^1 e^{-\lambda' N^{7/16}}\ \ln(\sqrt{N}\,\lambda')\,d\lambda'\right| \\
&\quad + O(\log N)\int_{N_1}^{N_2} s^2\,e^{-s^2/N}\left(\int_0^1\int_0^1(\lambda+\lambda')\,\ln(\sqrt{N}\,\lambda')\,e^{-(\lambda+\lambda')s}\right)d\lambda'\,d\lambda\,ds \\
&\quad + O\left((\log N)\,N^{-7/16}\right)\int_{N_1'}^{N_2'} s^2\,e^{-s^2/N} \\
&\qquad \times\left(\int_0^1\int_0^1 \ln(\sqrt{N}\,\lambda')\,e^{-(\lambda+\lambda')s}\,d\lambda' d\lambda\right)ds\ .
\end{aligned}
\tag{64}
$$

Now,

$$
\left|\int_0^1 e^{-\lambda N^{7/16}}\,d\lambda\right| = O(N^{-7/16})\ , \tag{65}
$$

and

$$\left|\int_0^1 e^{-\lambda' N^{7/16}} \ln(\sqrt{N}\,\lambda')d\lambda'\right| = O\Big(\int_0^1 e^{-\lambda' N^{7/16}} \ln(N^{7/16}\lambda')\,d\lambda' + (\log N)\int_0^1 e^{-\lambda' N^{7/16}}\,d\lambda'\Big)$$
$$= O\Big(N^{-7/16}\int_0^\infty e^{-x}\ln x\,dx + N^{-7/16}\log N\Big)$$
$$= O\Big(N^{-7/16}\log N\Big)\ . \qquad (66)$$

Also, for $N_1' \le s < N_2'$,

$$\left|\int_0^1\int_0^1 (\lambda+\lambda')\ln(\sqrt{N}\,\lambda')\,e^{-(\lambda+\lambda')s}\,d\lambda'\,d\lambda\right|$$
$$\le \left|\int_0^1 \lambda\, e^{-\lambda s}\,d\lambda \int_0^1 \ln(\sqrt{N}\,\lambda')\,e^{-\lambda' s}\,d\lambda'\right|$$
$$+\left|\int_0^1 e^{-\lambda s}\,d\lambda\int_0^1 \lambda' \ln(\sqrt{N}\,\lambda')\,e^{-\lambda' s}\,d\lambda'\right|$$
$$= O\Big(\frac{1}{s^2}\int_0^\infty x\,e^{-x}\,dx\cdot\frac{1}{s}\int_0^\infty \ln\Big(\frac{\sqrt{N}}{s}y\Big)\,e^{-y}\,dy\Big)$$
$$+\,O\Big(\frac{1}{s}\int_0^\infty e^{-x}\,dx\cdot\frac{1}{s^2}\int_0^\infty y\ln\Big(\frac{\sqrt{N}}{s}y\Big)\,e^{-y}\,dy\Big)$$
$$= O\Big(\frac{1}{s^3}\log N\Big)\ . \qquad (67)$$

Similarly, for $N_1' \le s < N_2'$

$$\left|\int_0^1\int_0^1 \ln(\sqrt{N}\,\lambda')\,e^{-(\lambda+\lambda')s}\,d\lambda'\,d\lambda\right| = \left|\int_0^1 e^{-\lambda s}\,d\lambda\right|\cdot\left|\int_0^1 \ln(\sqrt{N}\,\lambda')\,e^{-\lambda' s}\,d\lambda'\right|$$
$$= O\Big(\frac{1}{s^2}\log N\Big)\ . \qquad (68)$$

Using (65)-(68), we obtain from (64) that

$$L_2 = O\Big(e^{-N^{2\epsilon}}N^{1+2\epsilon}(\log N)^2\Big) + O\Big((\log N)\,N^{7/8}\,N^{-7/16}\,N^{-7/16}\log N\Big)$$
$$+\,O(\log N)\int_{N_1'}^{N_2'} s^2\,e^{-s^2/N}\,\frac{\log N}{s^3}\,ds$$
$$+\,O\Big((\log N)\,N^{-7/16}\Big)\int_{N_1'}^{N_2'} s^2\,e^{-s^2/N}\,\frac{1}{s^2}\log N\,ds$$
$$= O\Big((\log N)^2\Big) + O\Big((\log N)^2\,N^{-7/16}\int_0^\infty e^{-s^2/N}\,ds\Big)$$
$$= O\Big(N^{1/16}(\log N)^2\Big)\ . \qquad (69)$$

From (63) and (69), we obtain

$$\sum_{1\le k<N_3} H_k \int_0^1\int_0^1 \sum_{N_1\le m<N_2} e^{-m^2/N}\,\hat{h}_{N,m}(\lambda,\lambda',k)\ln(\sqrt{N}\,\lambda')\,d\lambda'\,d\lambda$$

$$= \sum_{1\le k<N_3} H_k \int_0^1 \int_0^1 \int_{N_1'}^{N_2'} \frac{(\lambda\lambda' N)^k}{k!} e^{-\lambda\lambda' N} s^2 e^{-(\lambda+\lambda')s - s^2/N} \ln(\sqrt{N}\,\lambda') d\lambda'\, d\lambda$$
$$+ O\Big(N^{1/16} (\log N)^2\Big)$$
$$= \sum_{1\le k<N_3} \frac{H_k}{k!} \int_0^{\sqrt{N}} \int_0^{\sqrt{N}} \int_{x_1}^{x_2} (uv)^k e^{-uv} N x^2 e^{-(u+v)x - x^2} (\ln v) \frac{dx\, dv\, du}{\sqrt{N}}$$
$$+ O\Big(N^{1/16} (\log N)^2\Big)$$
$$= \sqrt{N} \sum_{1\le k<N_3} H_k \int_0^{\sqrt{N}} \int_0^{\sqrt{N}} \int_{x_1}^{x_2} \psi_{1,k}(x,u,v)\, dx\, dv\, du$$
$$+ O\Big(N^{1/16} (\log N)^2\Big) \ . \tag{70}$$

This last expression is equal to, by Lemma 35,

$$\sqrt{N}\Big(\sum_{1\le k<N_3} H_k \beta_{1,k} + (\log N)^2 \cdot O(\frac{1}{\sqrt{N}} + e^{-x_2} + \sqrt{x_1})\Big) + O\Big(N^{1/16} (\log N)^2\Big)$$
$$= \sqrt{N}\Big\{ ((H_k)) + O(\frac{\log N}{\sqrt{N_3}}) + (\log N)^2 \cdot O(\frac{1}{\sqrt{N}} + e^{-x_2} + \sqrt{x_1})\Big\} + O\Big(N^{1/16} (\log N)^2\Big)$$
$$= \sqrt{N}\, ((H_k)) + O\Big(N^{15/32} (\log N)^2\Big) \ .$$

This proves Lemma 40. □

From (56), Lemma 39 and Lemma 40, we obtain

$$T_N + 2\, W_N \;=\; \sqrt{N}\Big((\gamma+1) << H_k >> - << H_k^2 >> - << H_k^{(2)} >> + 2\, ((H_k)) \Big)$$
$$+ \; O\Big(N^{1/2-\kappa} \log N\Big) \ . \tag{71}$$

Now, from Lemma 36, we have

$$(\gamma+1) << H_k >> - << H_k^2 >> - << H_k^{(2)} >> + 2((H_k))$$
$$= \sqrt{\pi} - \frac{\sqrt{\pi}}{2} \sum_{m\ge 1} \frac{4^m ((m-1)!)^2}{(2m+1)!} - \sqrt{\pi} \sum_{m\ge 1} \frac{1}{m} \frac{1}{(2m+1)^2}$$
$$= \frac{3}{4} \alpha \ .$$

Thus, we conclude

$$T_N + 2\, W_N = \frac{3}{4}\, \alpha \sqrt{N} + O\Big(N^{1/2-\kappa} \log N\Big) \ . \tag{72}$$

Theorem 3 follows immediately from (46) and (72).

Appendix A: Proof of Lemmas 24-30.

In the proofs of Lemma 24 and Lemmas 27-30 below, we will, without loss of generality, implicitly assume that N is sufficiently large such that $N_2 \le N/7$ and $(\ln N)/N_1 \le 1/30$. This ensures that $N - 2m > 0$ and $0 < a(m, N) < 1$, and we can structure our proof on that basis without further explanation.

A.1 Proof of Lemma 24.

For $1 \le m \le \lceil N_2 \rceil$, we have from Stirling's formula (see e.g. [K2, Section 1.2.11.2]) that

$$\begin{aligned}
\ln p_{N,m} &= 2\ln((N-m)!) - \ln((N-2m)!) - \ln(N!) \\
&= 2\Big(N - m + \frac{1}{2}\Big)\ln(N-m) - 2(N-m) + \ln(2\pi) + O\Big(\frac{1}{N-m}\Big) \\
&\quad - \Big(N - 2m + \frac{1}{2}\Big)\ln(N-2m) + (N-2m) - \frac{1}{2}\ln(2\pi) + O\Big(\frac{1}{N-2m}\Big) \\
&\quad - \Big(N + \frac{1}{2}\Big)\ln N + N - \frac{1}{2}\ln(2\pi) + O\Big(\frac{1}{N}\Big) \\
&= (2N - 2m + 1)\ln\Big(1 - \frac{m}{N}\Big) - \Big(N - 2m + \frac{1}{2}\Big)\ln\Big(1 - \frac{2m}{N}\Big) + O\Big(\frac{1}{N}\Big) \\
&= -\frac{m^2}{N} + O\Big(\frac{m^3}{N^2}\Big) + O\Big(\frac{1}{N}\Big) \ .
\end{aligned}$$

Thus,

$$\ln p_{N,m} = -\frac{m^2}{N} + O\Big(N^{-\frac{1}{2}+3\epsilon}\Big) \ . \tag{73}$$

For $N_2 \le m \le N - 2$, we observe that $p_{N,m} \le p_{N,\lceil N_2 \rceil}$, and that formula (73) gives $p_{N,\lceil N_2 \rceil} = O\Big(e^{-N^{2\epsilon}}\Big)$. This proves Lemma 24.

A.2 Proof of Lemma 25.

Let $g(x) = x^k\, e^{-x^2/N}$. Then, $g'(x) = \Big(\frac{k}{x} - \frac{2x}{N}\Big)\, g(x)$. Using Euler's Summation Formula (see e.g. [K2, Section 1.2.11.2]), we obtain, with $B_1(z) = z - 1/2$,

$$\begin{aligned}
\sum_{m\ge 1} m^k\, e^{-m^2/N} &= \sum_{m \ge 1} g(m) \\
&= \int_1^\infty g(x)\, dx - \frac{1}{2}(g(\infty) - g(1)) + \int_1^\infty B_1(x - \lfloor x \rfloor)\, g'(x)\, dx \\
&= \int_1^\infty N^{k/2}\, y^k\, e^{-y^2}\, N^{1/2}\, dy + O(1) + O\bigg(\int_1^\infty |g'(x)|\, dx\bigg) \\
&= O\Big(N^{(k+1)/2}\Big) + O\bigg(k \int_1^\infty x^{k-1}\, e^{-x^2/N}\, dx + \frac{1}{N}\int_1^\infty x^{k+1}\, e^{-x^2/N}\, dx\bigg) \\
&= O\Big(N^{(k+1)/2}\Big) \ .
\end{aligned}$$

This proves Lemma 25.

A.3 Proof of Lemma 26.

Clearly, $\sum_{0\leq k\leq N-2m} h_{N,m}(\lambda,\lambda',k) = m^2(1-\lambda)^{m-1}(1-\lambda')^{m-1}$, and $\sum_{k\geq 0} \hat{h}_{N,m}(\lambda,\lambda',k) = m^2\, e^{-(\lambda+\lambda')m}$. Hence,

$$\sum_{0\leq k\leq N-2m} \int_0^1 \int_0^1 h_{N,m}(\lambda,\lambda',k)\, d\lambda\, d\lambda' = \left(\int_0^1 m(1-\lambda)^{m-1}\, d\lambda\right)^2 = 1 \ .$$

It also follows that, for any $A > 0$,

$$\sum_{0\leq k\leq A} \int_0^1 \int_0^1 \hat{h}_{N,m}(\lambda,\lambda',k)\, d\lambda\, d\lambda' \leq \left(\int_0^1 m\, e^{-\lambda m}\, d\lambda\right)^2 \leq 1 \ ,$$

from which we conclude that

$$\sum_{k\geq 0} \int_0^1 \int_0^1 \hat{h}_{N,m}(\lambda,\lambda',k)\, d\lambda\, d\lambda' \leq 1 \ .$$

This proves Lemma 26.

A.4 Proof of Lemma 27.

By definition,

$$\begin{aligned} \ln h_{N,m}(\lambda,\lambda',k) = 2\ln m \quad &+ \quad \ln\binom{N-2m}{k} + (m-1)\ln(1-\lambda) + (m-1)\ln(1-\lambda') \\ &+ \quad k\ln(\lambda\lambda') + (N-2m-k)\ln(1-\lambda\lambda') \ . \end{aligned} \tag{74}$$

Now,

$$\begin{aligned} (m-1)\ln(1-\lambda) \quad &= \quad -\, m\lambda + O\Big(\lambda + m\lambda^2\Big) \\ &= \quad -\, m\lambda + O\Big((\log N)^2\, N^{-7/16}\Big) \ , \end{aligned} \tag{75}$$

and, similarly,

$$(m-1)\ln(1-\lambda') = -\, m\lambda' + O\Big((\log N)^2\, N^{-7/16}\Big) \ . \tag{76}$$

Also, we have

$$\begin{aligned} (N-2m-k)\ln(1-\lambda\lambda') \quad &= \quad -\, \lambda\lambda'(N-2m-k) + O\Big(N(\lambda\lambda')^2\Big) \\ &= \quad -\, \lambda\lambda' N + O\Big((\log N)^2\, N^{-7/16}\Big) \ . \end{aligned} \tag{77}$$

From Stirling's formula, we have

$$
\begin{aligned}
\ln\binom{N-2m}{k} &= \ln((N-2m)!) - \ln(k!) - \ln((N-2m-k)!) \\
&= \Big(N-2m+\frac{1}{2}\Big)\ln(N-2m) - (N-2m) + \frac{1}{2}\ln(2\pi) + O\Big(\frac{1}{N-2m}\Big) \\
&\quad - \Big(N-2m-k+\frac{1}{2}\Big)\ln(N-2m-k) + (N-2m-k) \\
&\quad - \frac{1}{2}\ln(2\pi) + O\Big(\frac{1}{N-2m-k}\Big) - \ln(k!) \\
&= -k - \ln(k!) + k\ln N + \Big(N-2m+\frac{1}{2}\Big)\ln\Big(1-\frac{2m}{N}\Big) \\
&\quad - \Big(N-2m+\frac{1}{2}-k\Big)\ln\Big(1-\frac{2m+k}{N}\Big) + O\Big(\frac{1}{N}\Big) \\
&= -\ln(k!) + k\ln N + O\Big(N^{-3/16+\epsilon}\Big) \qquad (78)
\end{aligned}
$$

It follows from (74) - (78) that

$$\ln h_{N,m}(\lambda,\lambda',k) = 2\ln m - \ln(k!) + k\ln N - m(\lambda+\lambda') + k\ln(\lambda\lambda') - \lambda\lambda' N + O\Big(N^{-1/8}\Big) \ .$$

Hence,

$$h_{N,m}(\lambda,\lambda',k) = \Big(1+O(N^{-1/8})\Big)\frac{(\lambda\lambda' N)^k}{k!}\, e^{-\lambda\lambda' N}\, m^2\, e^{-(\lambda+\lambda')m} \ .$$

This proves Lemma 27.

A.5 Proof of Lemma 28.

Using Lemma 26, we have

$$
\begin{aligned}
&\left|\int_0^1\int_0^1 h_{N,m}(\lambda,\lambda',k)\,d\lambda\,d\lambda' - \int_0^{a(m,N)}\int_0^{a(m,N)} h_{N,m}(\lambda,\lambda',k)\right| \\
&\le 2\int_0^1\int_{a(m,N)}^1 h_{N,m}(\lambda,\lambda',k)\,d\lambda\,d\lambda' \\
&\le 2\int_0^1\int_{a(m,N)}^1 m^2(1-\lambda)^{m-1}(1-\lambda')^{m-1}\,d\lambda\,d\lambda' \\
&= 2m\int_0^1 (1-\lambda)^{m-1}\,d\lambda \int_{a(m,N)}^1 m(1-\lambda')^{m-1}\,d\lambda' \\
&= 2(1-a(m,N))^m \\
&\le 2e^{-ma(m,N)} \\
&= 2e^{-10\ln N} \\
&= O(N^{-10}) \ .
\end{aligned}
$$

Similarly, we have

$$\left|\int_0^1\int_0^1 \hat{h}_{N,m}(\lambda,\lambda',k)\,d\lambda\,d\lambda' - \int_0^{a(m,N)}\int_0^{a(m,N)} \hat{h}_{N,m}(\lambda,\lambda',k)\,d\lambda\,d\lambda'\right|$$

$$\begin{aligned}
&\leq 2\int_0^1\int_{a(m,N)}^1 \hat{h}_{N,m}(\lambda,\lambda',k)\,d\lambda\,d\lambda' \\
&\leq 2\int_0^1\int_{a(m,N)}^1 m^2\,e^{-(\lambda+\lambda')m}\,d\lambda\,d\lambda' \\
&= 2\int_0^1 m\,e^{-\lambda m}\,d\lambda \int_{a(m,N)}^1 m\,e^{-\lambda' m}\,d\lambda' \\
&\leq 2\left(e^{-a(m,N)m} - e^{-m}\right) \\
&= O(N^{-10})\ .
\end{aligned}$$

This proves Lemma 28.

A.6 Proof of Lemma 29.

For $0 < \lambda, \lambda' \leq a(m,N)$, we have

$$\begin{aligned}
h_{N,m}(\lambda,\lambda',k) &\leq \binom{N-2m}{k}(\lambda\lambda')^k\,N^2 \\
&= O\left(\left(\frac{eN}{k}\right)^k (\lambda\lambda')^k\,N^2\right) \\
&= O\left(\left(\frac{e\,N}{N^{5/16}}\,\frac{100\,(\ln N)^2}{m^2}\right)^k N^2\right) \\
&= O\left(\left(\frac{100\,e(\ln N)^2}{N^{3/16}}\right)^k N^2\right) \\
&= O\left(2^{-N^{5/16}}\right)\ .
\end{aligned}$$

Thus, using Lemma 28, we have

$$\begin{aligned}
\int_0^1\int_0^1 h_{N,m}(\lambda,\lambda',k)\,d\lambda\,d\lambda' &= \int_0^{a(m,N)}\int_0^{a(m,N)} h_{m,N}(\lambda,\lambda',k)\,d\lambda\,d\lambda' + O(N^{-10}) \\
&= O\left(2^{-N^{5/16}}\right) + O(N^{-10}) \\
&= O(N^{-10})\ .
\end{aligned}$$

Similarly, for $0 < \lambda,\ \lambda' \leq a(m,N)$, we have

$$\begin{aligned}
\hat{h}_{N,m}(\lambda,\lambda',k) &\leq \left(\frac{e\lambda\lambda' N}{k}\right)^k N^2 \\
&= O\left(2^{-N^{5/16}}\right)\ ,
\end{aligned}$$

and then, using Lemma 28, we obtain

$$\begin{aligned}\int_0^1\int_0^1 \hat{h}_{N,m}(\lambda,\lambda',k)\,d\lambda\,d\lambda' &= \int_0^{a(m,N)}\int_0^{a(m,N)} \hat{h}_{N,m}(\lambda,\lambda',k)\,d\lambda\,d\lambda' + O(N^{-10})\\ &= O\Big(2^{-N^{5/16}}\Big) + O(N^{-10})\\ &= O(N^{-10})\ .\end{aligned}$$

This proves Lemma 29.

A.7 Proof of Lemma 30.

Let

$$\begin{aligned} I_j &= \Bigg| \sum_{1\le k<N_3} \int_0^1\int_0^1 F(k)f(\lambda,\lambda',k)(\ln(N\lambda'))^j\,d\lambda'\,d\lambda \\ &\quad - \sum_{1\le k<N_3}\int_0^{a(m,N)}\int_{b(m,N)}^{a(m,N)} F(k)f(\lambda,\lambda',k)(\ln(N\lambda'))^j\,d\lambda'\,d\lambda \Bigg|\ ,\end{aligned}$$

for $j\in\{0,1\}$. Clearly,

$$I_j \le M_{j1} + M_{j2} + M_{j3}\ , \tag{79}$$

where

$$M_{j1} = \sum_{1\le k<N_3}\int_{a(m,N)}^1\int_0^1 \left|F(k)f(\lambda,\lambda',k)(\ln(N\lambda'))^j\right| d\lambda'\,d\lambda\ , \tag{80}$$

$$M_{j2} = \sum_{1\le k<N_3}\int_0^{a(m,N)}\int_{a(m,N)}^1 \left|F(k)f(\lambda,\lambda',k)(\ln(N\lambda'))^j\right| d\lambda'\,d\lambda\ , \tag{81}$$

$$M_{j3} = \sum_{1\le k<N_3}\int_0^{a(m,N)}\int_0^{b(m,N)} \left|F(k)f(\lambda,\lambda',k)(\ln(N\lambda'))^j\right| d\lambda'\,d\lambda\ . \tag{82}$$

Note that, for $0<\lambda,\ \lambda'<1$, we have by Lemma 26

$$\sum_{1\le k<N_3} |f(\lambda,\lambda',k)| \le m^2\, e^{-(\lambda+\lambda')m+2}\ . \tag{83}$$

Using (83), we have

$$\begin{aligned} M_{j1} &= O((\log N)^2)\int_{a(m,N)}^1\int_0^1 m^2\,e^{-(\lambda+\lambda')m}\left|(\ln N+\ln\lambda')^j\right| d\lambda'\,d\lambda\\ &= O((\log N)^2)\Bigg\{\int_{a(m,N)}^1\int_0^1 (\ln N)\,m^2\,e^{-(\lambda+\lambda')m}\,d\lambda'\,d\lambda\\ &\qquad + \int_{a(m,N)}^1\int_0^1 \ln\Big(\frac{1}{\lambda'}\Big)m^2\,e^{-(\lambda+\lambda')m}\,d\lambda'\,d\lambda\Bigg\}\end{aligned}$$

$$
\begin{aligned}
&= O((\log N)^2)\Big\{(\ln N)\int_{a(m,N)}^{1} m\,e^{-\lambda m}\,d\lambda \int_0^1 m\,e^{-\lambda' m}\,d\lambda' \\
&\qquad + \int_{a(m,N)}^{1} m\,e^{-\lambda m}\,d\lambda \int_0^1 m\,e^{-\lambda' m}\,\ln\Big(\frac{1}{\lambda'}\Big)\,d\lambda'\Big\} \\
&= O((\log N)^2)\Big\{\Big(e^{-m\,a(m,N)}\Big)(\ln N + \ln m + 1)\Big\} \\
&= O(N^{-9}) \ . \qquad (84)
\end{aligned}
$$

Similarly, we have

$$
\begin{aligned}
M_{j2} &= O((\log N)^2)\int_0^1\int_{a(m,N)}^{1} m^2\,e^{-(\lambda+\lambda')m}\,\Big|(\ln N + \ln\lambda')^j\Big|\,d\lambda'\,d\lambda \\
&= O((\log N)^2)\Big\{\int_0^1\int_{a(m,N)}^{1} (\ln N)\,m^2\,e^{-(\lambda+\lambda')m}\,d\lambda'\,d\lambda \\
&\qquad + \int_0^1\int_{a(m,N)}^{1} \ln\Big(\frac{1}{\lambda'}\Big)m^2\,e^{-(\lambda+\lambda')m}\,d\lambda'\,d\lambda\Big\} \\
&= O((\log N)^2)\Big\{(\log N)\int_0^1 m\,e^{-\lambda m}\,d\lambda\int_{a(m,N)}^{1} m\,e^{-\lambda' m}\,d\lambda' \\
&\qquad + \int_0^1 m\,e^{-\lambda m}\,d\lambda\int_{a(m,N)}^{1} \ln\Big(\frac{1}{\lambda'}\Big)\,m\,e^{-\lambda' m}\,d\lambda'\Big\} \\
&= O((\log N)^2)\Big\{e^{-m\,a(m,N)}\,\ln N\Big\} \\
&= O(N^{-9}) \ . \qquad (85)
\end{aligned}
$$

The same approach gives

$$
\begin{aligned}
M_{03} &= O((\log N)^2)\int_0^1\int_0^{b(m,N)} m^2\,e^{-(\lambda+\lambda')m}\,d\lambda' d\lambda \\
&= O\Big((\log N)^2\Big)\cdot\Big(1-e^{-m}\Big)\Big(1-e^{-b(m,N)m}\Big) \\
&= O\Big((\log N)^2\cdot\Big(1-e^{-1/N^{1/10}}\Big)\Big) \\
&= O\Big((\log N)^2\,N^{-1/10}\Big) \ , \qquad (86)
\end{aligned}
$$

and

$$
\begin{aligned}
M_{13} &= O((\log N)^2)\int_0^1\int_0^{b(m,N)} m^2\,e^{-(\lambda+\lambda')m}\,\Big(\ln N + \ln\frac{1}{\lambda'}\Big)\,d\lambda' d\lambda \\
&= O((\log N)^2)\Big\{(\ln N)\int_0^1\int_0^{b(m,N)} m^2\,e^{-(\lambda+\lambda')m}\,d\lambda' d\lambda \\
&\qquad + \int_0^1\int_0^{b(m,N)} m^2\,e^{-(\lambda+\lambda')m}\,\ln\Big(\frac{1}{\lambda'}\Big)\,d\lambda' d\lambda\Big\} \\
&= O\Big((\log N)^3\,N^{-1/10}\Big) + O\Big((\log N)^2\Big)\int_0^{b(m,N)} m\,e^{-\lambda' m}\,\ln(\frac{1}{\lambda'})\,d\lambda' \ . \qquad (87)
\end{aligned}
$$

Now, for large N,

$$\begin{aligned}
\int_0^{b(m,N)} m\, e^{-\lambda' m} \ln(\frac{1}{\lambda'})\, d\lambda' &\leq \int_0^{mb(m,N)} e^{-x} \ln(\frac{m}{x})\, dx \\
&\leq (\ln m)\Big(1 - e^{-mb(m,N)}\Big) + \int_0^{N^{-1/10}} \ln\Big(\frac{1}{x}\Big)\, dx \\
&= O\Big((\log N)\, N^{-1/10}\Big) + (x - x\ln x)\,\Big|_{x=0}^{x=N^{-1/10}} \\
&= O\Big(N^{-1/10} \log N\Big)\ . \qquad (88)
\end{aligned}$$

From (87) and (88), we have

$$M_{13} = O\Big((\log N)^3\, N^{-1/10}\Big)\ . \qquad (89)$$

Lemma 30 follows from (79), (84)-(86), and (89).

Appendix B: Proof of Lemmas 31-34.

As in Appendix A, we will assume, without loss of generality, that N is sufficiently large such that $N_2 \le N/7$ and $(\ln N)/N_1 \le 1/30$ in the proofs of Lemma 32 and Lemma 33 below.

B.1 Proof of Lemma 31.

Immediate from the definitions.

B.2 Proof of Lemma 32.

Let

$$\begin{aligned} L = \Bigg| & \sum_{1\le k<N_3} \sum_{\ell\ge 1} \int_0^1 \int_0^1 \int_0^1 F(k,\ell)\, h_{N,m}(\lambda,\lambda',k) q_{N,m,k,\ell}(\lambda,\lambda',z)\, dz\, d\lambda'\, d\lambda \\ & - \sum_{1\le k<N_3} \sum_{\ell\ge 1} \int_0^{a(m,N)} \int_{b(m,N)}^{a(m,N)} \int_{N^{-3/8}}^1 F(k,\ell) h_{N,m}(\lambda,\lambda',k) \\ & \times q_{N,m,k,\ell}(\lambda,\lambda',z)\, dz\, d\lambda'\, d\lambda \Bigg| . \end{aligned}$$

Then,

$$L \le L_1 + L_2 + L_3 + L_4, \tag{90}$$

where

$$L_1 = \sum_{1\le k<N_3} \sum_{\ell\ge 1} \int_{a(m,N)}^1 \int_0^1 \int_0^1 |F(k,\ell)|\, h_{N,m}(\lambda,\lambda',k)\, q_{N,m,k,\ell}(\lambda,\lambda',z)\, dz\, d\lambda'\, d\lambda , \tag{91}$$

$$L_2 = \sum_{1\le k<N_3} \sum_{\ell\ge 1} \int_0^1 \int_{a(m,N)}^1 \int_0^1 |F(k,\ell)|\, h_{N,m}(\lambda,\lambda',k)\, q_{N,m,k,\ell}(\lambda,\lambda',z)\, dz\, d\lambda'\, d\lambda , \tag{92}$$

$$L_3 = \sum_{1\le k<N_3} \sum_{\ell\ge 1} \int_0^1 \int_0^{b(m,N)} \int_0^1 |F(k,\ell)|\, h_{N,m}(\lambda,\lambda',k)\, q_{N,m,k,\ell}(\lambda,\lambda',z)\, dz\, d\lambda'\, d\lambda , \tag{93}$$

and

$$L_4 = \sum_{1\le k<N_3} \sum_{\ell\ge 1} \int_0^1 \int_0^1 \int_0^{N^{-3/8}} |F(k,\ell)|\, h_{N,m}(\lambda,\lambda',k)\, q_{N,m,k,\ell}(\lambda,\lambda',z)\, dz\, d\lambda'\, d\lambda , \tag{94}$$

From Lemmas 31 and 26, we obtain

$$\begin{aligned} L_1 &= \sum_{1\le k<N_3} \int_{a(m,N)}^1 \int_0^1 O((\log N)^2)\, h_{N,m}(\lambda,\lambda',k)\, d\lambda'\, d\lambda \\ &= O((\log N)^2) \int_{a(m,N)}^1 \int_0^1 m^2 (1-\lambda)^{m-1}(1-\lambda')^{m-1}\, d\lambda'\, d\lambda . \end{aligned}$$

We have evaluated this expression in the proof of Lemma 28, which gives

$$L_1 = O\left(N^{-9}\right) . \tag{95}$$

A similar argument proves

$$L_2 = O\left(N^{-9}\right) . \tag{96}$$

To evaluate L_3, we obtain from Lemma 31

$$\begin{aligned} L_3 &= \sum_{1\le k<N_3} \int_0^1 \int_0^{b(m,N)} O((\log N)^2)\, h_{N,m}(\lambda,\lambda',k)\, d\lambda'\, d\lambda \\ &= O((\log N)^2) \int_0^1 \int_0^{b(m,N)} m^2\,(1-\lambda)^{m-1}(1-\lambda')^{m-1}\, d\lambda'\, d\lambda \\ &= O((\log N)^2) \int_0^1 \int_0^{b(m,N)} m^2\, e^{-(\lambda+\lambda')m}\, d\lambda'\, d\lambda \ . \end{aligned}$$

We have evaluated this expression in the derivation of (87), which gives

$$L_3 = O\left((\log N)^2\, N^{-1/10}\right) . \tag{97}$$

To evaluate L_4, observe that

$$\begin{aligned} \int_0^{N^{-3/8}} \sum_{\ell\ge 1} q_{N,m,k,\ell}(\lambda,\lambda',z)\,|F(k,\ell)|\, dz &= O((\log N)^2) \int_0^{N^{-3/8}} k\,(1-z)^{k-1}\, dz \\ &= O((\log N)^2)\left(1-(1-N^{-3/8})^k\right) \\ &= O\left((\log N)^2\left(1-e^{O(k\,N^{-3/8})}\right)\right) \\ &= O\left((\log N)^2\, N^{-1/16}\right) . \end{aligned}$$

Thus, from (94) and Lemma 26, we obtain

$$\begin{aligned} L_4 &= O\left((\log N)^2\, N^{-1/16}\right) \sum_{1\le k<N_3} \int_0^1 \int_0^1 h_{N,m}(\lambda,\lambda',k)\, d\lambda'\, d\lambda \\ &= O\left((\log N)^2\, N^{-1/16}\right) . \end{aligned} \tag{98}$$

Lemma 32 follows from (90), (95)-(98).

B.3 Proof of Lemma 33.

Let $y = \lambda'(1-\lambda)z/(1-\lambda\lambda')$, and $M = N - 2m - k$. Then

$$q_{N,m,k,\ell}(\lambda,\lambda',z) = k(1-z)^{k-1}\binom{M}{\ell}\, y^\ell\,(1-y)^{M-\ell} . \tag{99}$$

Let $K = \sum_{\ell \geq 1} H_\ell \binom{M}{\ell} y^\ell (1-y)^{M-\ell}$. Then

$$\sum_{\ell \geq 1} H_\ell \, q_{N,m,k,\ell}(\lambda, \lambda', z) = k(1-z)^{k-1} K \ . \tag{100}$$

Now, consider the flip of M independent coins, each having probability y to be a "TAIL". Then, $\binom{M}{\ell} y^\ell (1-y)^{M-\ell}$ is the probability that exactly ℓ "TAIL" will occur, and K is the expected value of the quantity H_ℓ. To evaluate K, we show that the probability that ℓ differs significantly from the expected value yM is small, which gives $K \approx \ln(yM)$.

Let $\epsilon' = 1/700$. In the range of parameters considered, it is easy to see that for large enough N,

$$N^{-39/40+\epsilon'} < y < 20(\ln N)\, N^{-7/16} \ . \tag{101}$$

Let $\delta = \sum_{|\ell - yM| > (yM)^{3/4}} \binom{M}{\ell} y^\ell (1-y)^{M-\ell}$. In terms of the experiment of flipping M independent coins of bias y, we have

$$\delta = \Pr\left\{ \left| \frac{\ell}{M} - y \right| > \tau \right\} , \tag{102}$$

where $\tau = y^{3/4}/M^{1/4}$. A well-known inequality (see Rényi [R, eq. 4.4.18]) gives, for large N,

$$\begin{aligned} \delta &\leq 2\, e^{-M\tau^2/(4y(1-y))} \\ &\leq 2\, e^{-\sqrt{My}/4} \\ &\leq 2^{-N^{0.01}} \ . \end{aligned} \tag{103}$$

Observe that, for ℓ satisfying $|\ell - yM| \leq (yM)^{3/4}$,

$$\ell = yM\left(1 + O\Big(\frac{1}{(yM)^{1/4}}\Big)\right) ,$$

and hence,

$$\begin{aligned} H_\ell &= \ln \ell + \gamma + O\Big(\frac{1}{\ell}\Big) \\ &= \ln(yM) + \gamma + O\Big(\frac{1}{(yM)^{1/4}}\Big) \\ &= \ln(N\lambda' z) + \gamma + O(\lambda) + O(N^{-1/2+\epsilon'}) + O\Big(\frac{1}{(yN)^{1/4}}\Big) \ . \end{aligned} \tag{104}$$

From (101), (104), and the bounds on the range of λ, we have , for ℓ in this range,

$$H_\ell = \ln(N\lambda' z) + \gamma + O(N^{-1/200}) \ . \tag{105}$$

Using (103) and (105), we obtain

$$\begin{aligned} K &= (1-\delta)\Big(\ln(N\lambda' z)+\gamma+O(N^{-1/200})\Big)+\delta\cdot O(\ln N) \\ &= \ln(N\lambda' z)+\gamma+O(N^{-1/200}) \ . \end{aligned} \tag{106}$$

Lemma 33 follows from (100) and (106).

B.4 Proof of Lemma 34.

It is elementary that, for large N

$$\begin{aligned} \int_{N^{-3/8}}^{1} k(1-z)^k\,dz &= (1-N^{-3/8})^k \\ &\geq e^{-2kN^{-3/8}} \\ &\geq 1-2k\,N^{-3/8} \\ &\geq 1-2N_3\,N^{-3/8} \\ &= 1-2N^{-1/16} \ . \end{aligned}$$

As $\int_{N^{-3/8}}^1 k(1-z)^{k-1}\,dz \leq \int_0^1 k(1-z)^{k-1}\,dz = 1$, we have

$$\int_{N^{-3/8}}^{1} k(1-z)^{k-1}\,dz = 1-O(N^{-1/16}) \ . \tag{107}$$

This proves one of the inequalities in Lemma 34.

Let $1/N < \delta < 1$, then

$$\begin{aligned} \left|\int_0^\delta k(1-z)^{k-1}\ln z\,dz\right| &\leq \left|\int_0^{1/N} k(1-z)^{k-1}\ln z\,dz\right| + \left|\int_{1/N}^{\delta} k(1-z)^{k-1}\ln z\,dz\right| \\ &\leq k\left|\int_0^{1/N}\ln z\,dz\right| + (\ln N)\int_{1/N}^{\delta} k(1-z)^{k-1}dz \\ &= O\Big(k(\ln N)/N\Big)+O(k\,\delta\ln N) \ . \end{aligned}$$

It follows that

$$\left|\int_0^{N^{-3/8}} k(1-z)^{k-1}\ln z\,dz\right| = O\Big(N^{-1/16}(\log N)\Big) \ . \tag{108}$$

Let $0 < w < 1$ be any number. Then the following expansion is uniformly convergent for $|z| < w$:

$$\ln(1-z) = -\sum_{m\geq 1}\frac{1}{m}z^m \ . \tag{109}$$

It follows that, for any $0 < w < 1$, we have

$$\begin{aligned} \int_0^w k\,z^{k-1}\ln(1-z)\,dz &= -\sum_{m\geq 1}\int_0^w k\,z^{k-1}\,\frac{1}{m}\,z^m\,dz \\ &= -\sum_{m\geq 1}\frac{k}{m}\,\frac{1}{m+k}\,w^{m+k} \ . \end{aligned}$$

The infinite series of functions (of the variable w) on the right-hand side of the above expression is uniformly convergent on the interval [0, 1]. We can thus interchange limit and summation (see [A, Theorem 9.7]). Thus,

$$\begin{aligned}\int_0^1 k\, z^{k-1} \ln(1-z)\, dz &= -\lim_{w \to 1-} \sum_{m \geq 1} \frac{k}{m} \frac{1}{m+k} w^{m+k} \\ &= -\sum_{m \geq 1} \frac{k}{m} \frac{1}{m+k} \\ &= -H_k \ . \end{aligned} \tag{110}$$

From (108) and (110), we obtain

$$\int_{N^{-3/8}}^1 k(1-z)^{k-1} \ln z\, dz = -H_k + O\Big(N^{-1/16}(\log N)\Big) \ . \tag{111}$$

This completes the proof of Lemma 34.

Appendix C: Proof of Lemmas 35-36.

C.1 Proof of Lemma 35.

(a) Note that $\psi_{0,k}(x,u,v) \geq 0$ for all $k \geq 1$, $x,u,v \geq 0$; $\psi_{1,k}(x,u,v) \geq 0$ if $v \geq 1$ and $\psi_{1,k}(x,u,v) < 0$ if $0 < v < 1$. To show that $\beta_{j,k}$ exists, we only need to prove that there exist two constants $C_1, C_2 > 0$ such that, for all $r_1, r_2 > 0$ and $r_3 > 1$,

$$\int_0^{r_1}\int_0^{r_2}\int_1^{r_3} |\psi_{j,k}(x,u,v)|\, dv\, du\, dx \leq C_1 \ , \tag{112}$$

and

$$\int_0^{r_1}\int_0^{r_2}\int_0^{1} |\psi_{j,k}(x,u,v)|\, dv\, du\, dx \leq C_2 \ . \tag{113}$$

To prove (112), we observe that

$$\begin{aligned}
&\int_0^{r_1}\int_0^{r_2}\int_1^{r_3} |\psi_{j,k}(x,u,v)|\, dv\, du\, dx \\
&\quad \leq \int_0^{r_1}\int_0^{r_2}\int_1^{r_3} x^2\, e^{-x^2-(u+v)x}\, (\ln v)^j\, dv\, du\, dx \\
&\quad = \int_0^{r_1} e^{-x^2}\left\{\int_0^{r_2} x\, e^{-ux}\, du\right\}\left\{\int_1^{r_3} x e^{-vx}\, (\ln v)^j\, dv\right\} dx \\
&\quad \leq \int_0^{r_1} e^{-x^2}\left\{\int_x^{r_3 x} e^{-y}(\ln y - \ln x)^j\, dy\right\} dx \\
&\quad \leq \int_0^{\infty} e^{-x^2}\, dx \int_0^{\infty} e^{-y}(1+|\ln y|)\, dy + \int_0^{\infty} |\ln x|\, e^{-x^2}\, dx \ .
\end{aligned}$$

This proves (112).

Now, note that

$$\begin{aligned}
&\int_0^{r_1}\int_0^{r_2}\int_0^{1} |\psi_{j,k}(x,u,v)|\, dv\, du\, dx \\
&\quad \leq \int_0^{r_1}\int_0^{r_2}\int_0^{1} x^2\, e^{-x^2-(u+v)x}\, \left(\ln(1/v)\right)^j\, dv\, du\, dx \\
&\quad \leq \int_0^{r_1} e^{-x^2}\left\{\int_0^{r_2} x\, e^{-ux}\, du\right\}\left\{\int_0^{1} x\, e^{-vx}\, \left(\ln(1/v)\right)^j\, dv\right\} dx \\
&\quad \leq \int_0^{r_1} e^{-x^2}\left\{\int_0^{x} e^{-y}(1+|\ln y|+|\ln x|)\, dy\right\} dx \\
&\quad \leq \int_0^{\infty} e^{-x^2}\, dx \int_0^{\infty} e^{-y}(1+|\ln y|)\, dy + \int_0^{\infty} e^{-x^2}|\ln x|\, dx \ .
\end{aligned}$$

This proves (113), and completes the proof of item (a) in Lemma 35.

(b) Let

$$K_j = \left|\sum_{1\leq k\leq D} F(k)\int_{X_1}^{X_2}\int_0^{B}\int_1^{B} \psi_{j,k}(x,u,v)\, dv\, du\, dx\right.$$

$$- \sum_{1 \le k \le D} F(k) \int_0^\infty \int_0^\infty \int_1^\infty \psi_{j,k}(x,u,v)\, dv\, du\, dx \Bigg| \ ,$$

and

$$M_j = \Bigg| \sum_{1 \le k \le D} F(k) \int_{X_1}^{X_2} \int_0^B \int_0^1 \psi_{j,k}(x,u,v)\, dv\, du\, dx$$

$$- \sum_{1 \le k \le D} F(k) \int_0^\infty \int_0^\infty \int_0^1 \psi_{j,k}(x,u,v)\, dv\, du\, dx \Bigg| \ .$$

It suffices to prove that

$$K_j = O\left(\frac{C(D)(\log B)^j}{B} + e^{-X_2} C(D) + \sqrt{X_1}\, C(D) \right) \ , \tag{114}$$

and

$$M_j = O\left(\frac{C(D)(\log B)^j}{B} + e^{-X_2} C(D) + \sqrt{X_1}\, C(D) \right) \ . \tag{115}$$

Clearly,

$$K_j \le T_{1,j} + T_{2,j} + T_{3,j} + T_{4,j} \ , \tag{116}$$

where

$$T_{1,j} = \sum_{1 \le k \le D} F(k) \int_{X_2}^\infty \int_0^\infty \int_1^\infty \psi_{j,k}(x,u,v)\, dv\, du\, dx \ ,$$

$$T_{2,j} = \sum_{1 \le k \le D} F(k) \int_0^{X_1} \int_0^\infty \int_1^\infty \psi_{j,k}(x,u,v)\, dv\, du\, dx \ ,$$

$$T_{3,j} = \sum_{1 \le k \le D} F(k) \int_0^\infty \int_B^\infty \int_1^\infty \psi_{j,k}(x,u,v)\, dv\, du\, dx \ ,$$

and

$$T_{4,j} = \sum_{1 \le k \le D} F(k) \int_0^\infty \int_0^\infty \int_B^\infty \psi_{j,k}(x,u,v)\, dv\, du\, dx \ ,$$

Observe that

$$\begin{aligned}
|T_{1,j}| &\le C(D) \int_{X_2}^\infty \int_0^\infty \int_1^\infty x^2 e^{-x^2-(u+v)x} (\ln v)^j\, dv\, du\, dx \\
&\le C(D) \int_{X_2}^\infty e^{-x^2} \left\{ \int_0^\infty x e^{-ux}\, du \right\} \left\{ \int_1^\infty x e^{-vx} (\ln v)^j\, dv \right\} dx \\
&\le C(D) \int_{X_2}^\infty e^{-x^2} \left\{ \int_1^\infty e^{-y}(1 + \ln y + \ln x)\, dy \right\} dx \\
&= O\left(C(D) \int_{X_2}^\infty e^{-x^2}\, dx + C(D) \int_{X_2}^\infty (\ln x) e^{-x^2}\, dx \right) \\
&= O\left(e^{-X_2} C(D) \right) \ .
\end{aligned} \tag{117}$$

Similarly,

$$\begin{aligned}
|T_{2,j}| &\le C(D)\int_0^{X_1}\int_0^{\infty}\int_1^{\infty} x^2\, e^{-x^2-(u+v)x}\,(\ln v)^j\, dv\, du\, dx \\
&= O\Big(C(D)\int_0^{X_1} e^{-x^2}\, dx + C(D)\int_0^{X_1} |\ln x|\, e^{-x^2}\, dx\Big) \\
&= O\big(C(D)\, X_1\, \ln(e/X_1)\big) \\
&= O\big(C(D)\sqrt{X_1}\,\big)\ . \qquad (118)
\end{aligned}$$

We also have,

$$\begin{aligned}
|T_{3,j}| &\le C(D)\int_0^{\infty}\int_B^{\infty}\int_1^{\infty} x^2\, e^{-x^2-(u+v)x}\,(\ln v)^j\, dv\, du\, dx \\
&\le C(D)\int_0^{\infty} e^{-x^2}\left\{\int_B^{\infty} x\, e^{-ux}\, du\right\}\left\{\int_1^{\infty} x\, e^{-vx}\,(\ln v)^j\, dv\right\} dx \\
&\le C(D)\int_0^{\infty} e^{-x^2} e^{-Bx}\left\{\int_x^{\infty} e^{-y}(1+|\ln y|^j\,)\, dy + |\ln x|^j \int_x^{\infty} e^{-y}\, dy\right\} dx \\
&= O\Big(C(D)\int_0^{\infty} e^{-x^2-Bx}\, dx + C(D)\int_0^{\infty} e^{-x^2-Bx}\, |\ln x|^j\, dx\Big) \\
&= O\Big(\frac{C(D)}{B} + \frac{C(D)}{B}\,(\ln B)^j\Big)\ . \qquad (119)
\end{aligned}$$

Similarly,

$$\begin{aligned}
|T_{4,j}| &\le C(D)\int_0^{\infty}\int_0^{\infty}\int_B^{\infty} x^2\, e^{-x^2-(u+v)x}\,(\ln v)^j\, dv\, du\, dx \\
&\le C(D)\int_B^{\infty}(\ln v)^j \int_0^{\infty} x\, e^{-x^2-vx}\left\{\int_0^{\infty} x\, e^{-ux}\, du\right\} dx\, dv \\
&= O\Big(C(D)\int_B^{\infty}(\ln v)^j\left\{\int_0^{\infty} x\, e^{-vx}\, dx\right\} dv\Big) \\
&= O\Big(C(D)\int_B^{\infty}\frac{(\ln v)^j}{v^2}\, dv\Big) \\
&= \Big(C(D)\,\frac{(\ln B)^j}{B}\Big)\ . \qquad (120)
\end{aligned}$$

From (116) - (120), we obtain (114).

To prove (115), we can write

$$M_j \le L_{1,j} + L_{2,j} + L_{3,j}\ , \qquad (121)$$

where

$$L_{1,j} = \sum_{1\le k\le D} F(k)\int_{X_2}^{\infty}\int_0^{\infty}\int_0^1 |\psi_{j,k}(x,u,v)|\, dv\, du\, dx\ ,$$

$$L_{2,j} = \sum_{1\le k\le D} F(k) \int_0^{X_1} \int_0^{\infty} \int_0^1 |\psi_{j,k}(x,u,v)| \; dv\, du\, dx \quad ,$$

and

$$L_{3,j} = \sum_{1\le k\le D} F(k) \int_0^{\infty} \int_B^{\infty} \int_0^1 |\psi_{j,k}(x,u,v)| \; dv\, du\, dx \quad .$$

Now,

$$\begin{aligned}
|L_{1,j}| &\le C(D) \int_{X_2}^{\infty} \int_0^{\infty} \int_0^1 x^2\, e^{-x^2-(u+v)x} \ln\Big(\frac{1}{v}\Big)\, dv\, du\, dx \\
&= O\bigg(C(D) \int_{X_2}^{\infty} e^{-x^2} \Big\{ \int_0^1 x\, e^{-vx} \ln\Big(\frac{1}{v}\Big)\, dv \Big\}\, dx \bigg) \\
&= O\bigg(C(D) \int_{X_2}^{\infty} e^{-x^2} \Big\{ \int_0^x e^{-y} \Big(\ln x + |\ln y|\Big)\, dy \Big\}\, dx \bigg) \\
&= O\bigg(C(D) \int_{X_2}^{\infty} e^{-x^2} \ln x\, dx \bigg) \\
&= O\Big(C(D)\, e^{-X_2} \Big) \quad . \qquad (122)
\end{aligned}$$

Similarly,

$$\begin{aligned}
|L_{2,j}| &\le C(D) \int_0^{X_1} \int_0^{\infty} \int_0^1 x^2\, e^{-x^2-(u+v)x} \ln\Big(\frac{1}{v}\Big)\, dv\, du\, dx \\
&= O\bigg(C(D) \int_0^{X_1} e^{-x^2} \Big\{ \int_0^1 x\, e^{-vx} \ln\Big(\frac{1}{v}\Big)\, dv \Big\}\, dx \bigg) \\
&= O\bigg(C(D) \int_0^{X_1} e^{-x^2}\, x\, dx \bigg) \\
&= O\Big(C(D)\, X_1^2 \Big) \quad . \qquad (123)
\end{aligned}$$

It is also elementary that,

$$\begin{aligned}
|L_{3,j}| &\le C(D) \int_0^{\infty} \int_B^{\infty} \int_0^1 x^2\, e^{-x^2-(u+v)x} \ln\Big(\frac{1}{v}\Big)\, dv\, du\, dx \\
&= C(D) \int_0^{\infty} \int_B^{\infty} x^2\, e^{-x^2-ux} \Big\{ \int_0^1 e^{-vx} \ln\Big(\frac{1}{v}\Big)\, dv \Big\}\, du\, dx \\
&= O\bigg(C(D) \int_0^{\infty} \int_B^{\infty} x^2\, e^{-x^2-ux}\, du\, dx \bigg) \\
&= O\bigg(C(D) \int_B^{\infty} \Big\{ \int_0^{\infty} x^2\, e^{-ux}\, dx \Big\}\, du \bigg) \\
&= O\bigg(C(D) \int_B^{\infty} \frac{1}{u^3}\, du \bigg) \\
&= O\bigg(\frac{C(D)}{B^2} \bigg) \quad . \qquad (124)
\end{aligned}$$

Clearly, (115) follows from (121) - (124). This proves item (b) in the lemma.

(c) Let $k \geq 200$. We have

$$\begin{aligned}
\beta_{0,k} &= \frac{1}{k!}\int_0^\infty\int_0^\infty\int_0^\infty (uv)^k\, e^{-uv}\, x^2\, e^{-x^2-(u+v)x}\, dv\, du\, dx \\
&= \frac{1}{k!}\int_0^\infty\int_0^\infty (uv)^k\, e^{-uv}\left\{\int_0^\infty x^2\, e^{-(u+v)x}\, dx\right\} dv\, du \\
&= O\left(\frac{1}{k!}\int_0^\infty\int_0^\infty (uv)^k\, e^{-uv}\,\frac{1}{(u+v)^3}\, dv\, du\right) \\
&= O\left(\frac{1}{k!}\int_0^\infty\int_0^u (uv)^k\, e^{-uv}\,\frac{1}{(u+v)^3}\, dv\, du\right) \\
&= O\left(\frac{1}{k!}\int_0^\infty\int_0^u (uv)^k\, e^{-uv}\,\frac{1}{u^3}\, dv\, du\right) \\
&= O\left(\frac{1}{k!}\int_0^\infty \frac{1}{u^3}\left\{\int_0^{u^2} w^k\, e^{-w}\,\frac{1}{u}\, dw\right\} du\right) \\
&= O\left(\frac{1}{k!}\left(Q(0,\sqrt{k}/10) + Q(\sqrt{k}/10,\infty)\right)\right) \quad , \qquad (125)
\end{aligned}$$

where

$$Q(x,y) = \int_x^y \frac{1}{u^4}\left\{\int_0^{u^2} w^k\, e^{-w}\, dw\right\} du \quad . \qquad (126)$$

Now,

$$\begin{aligned}
Q(\sqrt{k}/10,\infty) &\leq \int_{\sqrt{k}/10}^\infty \frac{1}{u^4}\left\{\int_0^\infty w^k\, e^{-w}\, dw\right\} du \\
&= \int_{\sqrt{k}/10}^\infty \frac{1}{u^4}\, k!\, du \\
&= O\left(k!\, k^{-3/2}\right) \quad . \qquad (127)
\end{aligned}$$

Also,

$$\begin{aligned}
Q(0,\sqrt{k}/10) &\leq \int_0^{\sqrt{k}/10} \frac{1}{u^4}\left\{\int_0^{u^2} w^k\, dw\right\} du \\
&= \int_0^{\sqrt{k}/10} \frac{1}{u^4}\,\frac{u^{2(k+1)}}{k+1}\, du \\
&= \frac{1}{k+1}\,\frac{1}{2k-1}\left(\frac{\sqrt{k}}{10}\right)^{2k-1} \\
&= O\left(k!\, 2^{-k}\right) \quad . \qquad (128)
\end{aligned}$$

It follows from (125), (127) and (128) that, for $k \geq 1$,

$$\beta_{0,k} = O(k^{-3/2}) \quad . \qquad (129)$$

This proves one of the inequalities in item (c).

We now estimate $\beta_{1,k}$. Write

$$\beta_{1,k} = s_k - t_k \ , \tag{130}$$

where

$$s_k = \frac{1}{k!} \int_0^\infty \int_0^\infty \int_1^\infty (uv)^k \, e^{-uv} \, x^2 \, e^{-x^2-(u+v)x} \, (\ln v) \, dv \, du \, dx \ ,$$

and

$$t_k = \frac{1}{k!} \int_0^\infty \int_0^\infty \int_0^1 (uv)^k \, e^{-uv} \, x^2 \, e^{-x^2-(u+v)x} \, \ln(1/v) \, dv \, du \, dx \ .$$

Clearly,

$$\begin{aligned}
k! \, s_k &= \int_0^\infty \int_1^\infty (uv)^k \, e^{-uv} \, (\ln v) \left\{ \int_0^\infty x^2 \, e^{-x^2-(u+v)x} \, dx \right\} dv \, du \\
&= O\left(\int_0^\infty \int_1^\infty (uv)^k \, e^{-uv} \, (\ln v) \, \frac{1}{(u+v)^3} \, dv \, du \right) \\
&= O\left(\int_0^1 \int_1^\infty (uv)^k \, e^{-uv} \, (\ln v) \, \frac{1}{(u+v)^3} \, dv \, du \right. \\
&\qquad \left. + \frac{1}{2} \int_1^\infty \int_1^\infty (uv)^k \, e^{-uv} \, (\ln(uv)) \, \frac{1}{(u+v)^3} \, dv \, du \right) \\
&= O\left(\int_0^1 \int_1^\infty u^k \, v^{k-3} \, e^{-uv} \, (\ln v) \, dv \, du \right. \\
&\qquad \left. + \int_1^\infty \int_1^u (uv)^k \, e^{-uv} \, (\ln(uv)) \, \frac{1}{(u+v)^3} \, dv \, du \right) \ .
\end{aligned} \tag{131}$$

Note that

$$\begin{aligned}
\int_0^1 \int_1^\infty u^k \, v^{k-3} \, e^{-uv} (\ln v) \, dv \, du &= \int_1^\infty v^{k-3} (\ln v) \left\{ \int_0^1 u^k \, e^{-uv} \, du \right\} dv \\
&= \int_1^\infty v^{k-3} (\ln v) \, \frac{1}{v^{k+1}} \left\{ \int_0^v w^k \, e^{-w} \, dw \right\} dv \\
&= J(1, \sqrt{k}/10) + J(\sqrt{k}/10, \infty) \ ,
\end{aligned} \tag{132}$$

where

$$J(x,y) = \int_x^y \frac{\ln v}{v^4} \left\{ \int_0^v w^k \, e^{-w} \, dw \right\} dv \ .$$

It is easy to see that

$$\begin{aligned}
J(\sqrt{k}/10, \infty) &\leq \int_{\sqrt{k}/10}^\infty \frac{\ln v}{v^4} \left\{ \int_0^\infty w^k \, e^{-w} \, dw \right\} dv \\
&= \int_{\sqrt{k}/10}^\infty \frac{\ln v}{v^4} \, k! \, dv \\
&= O\Big(k! \, (\log k) \, k^{-3/2} \Big) \ ,
\end{aligned} \tag{133}$$

and that

$$
\begin{aligned}
J(1, \sqrt{k}/10) &\leq \int_1^{\sqrt{k}/10} \frac{\ln v}{v^4} \left\{ \int_0^v w^k \, dw \right\} dv \\
&= \int_1^{\sqrt{k}/10} \frac{\ln v}{v^4} \frac{v^{k+1}}{k+1} \, dv \\
&= O\left(\frac{1}{k+1} \left(\frac{\sqrt{k}}{10} \right)^{k-2} \frac{\log k}{k} \right) \\
&= O\left(k! \, 2^{-k} \right) . \qquad (134)
\end{aligned}
$$

From (132)-(134), we have

$$
\int_0^1 \int_1^\infty u^k \, v^{k-3} \, e^{-uv} \, (\ln v) \, dv \, du = O\left(k! \, (\log k) \, k^{-3/2} \right) . \qquad (135)
$$

We now analyze the other term in (131). It is clear that

$$
\begin{aligned}
&\int_1^\infty \int_1^u (uv)^k \, e^{-uv} \, (\ln(uv)) \, \frac{1}{(u+v)^3} \, dv \, du \\
&= O\left(\int_1^\infty \int_1^u u^{k-3} \, v^k \, e^{-uv} \ln u \, dv \, du \right) \\
&= O\left(\int_1^\infty u^{k-3} \ln u \left\{ \int_1^u v^k \, e^{-uv} \, dv \right\} du \right) \\
&= O\left(\int_1^\infty \frac{\ln u}{u^4} \left\{ \int_u^{u^2} w^k \, e^{-w} \, dw \right\} du \right) \\
&= O\left(\int_1^\infty \frac{\ln u}{u^4} \left\{ \int_0^{u^2} w^k \, e^{-w} \, dw \right\} du \right) \\
&= O\left(I(1, \sqrt{k}/10) + I(\sqrt{k}/10, \infty) \right) , \qquad (136)
\end{aligned}
$$

where

$$
I(x, y) = \int_x^y \frac{\ln u}{u^4} \left\{ \int_0^{u^2} w^k \, e^{-w} \, dw \right\} dw .
$$

We have evaluated similar expressions in the derivation of (125) previously. We can establish, similarly,

$$
\begin{aligned}
I(\sqrt{k}/10, \infty) &= \int_{\sqrt{k}/10}^\infty \frac{\ln u}{u^4} \, k! \, du \\
&= O\left((\log k) \, k^{-3/2} \cdot k! \right) , \qquad (137)
\end{aligned}
$$

and

$$
\begin{aligned}
I(1, \sqrt{k}/10) &= \int_1^{\sqrt{k}/10} \frac{\ln u}{u^4} \frac{u^{2(k+1)}}{k+1} \, du \\
&= O\left(\frac{\log k}{k+1} \left(\frac{\sqrt{k}}{10} \right)^{2k-1} \frac{1}{k} \right) \\
&= O\left(k! \, 2^{-k} \right) , \qquad (138)
\end{aligned}
$$

From (136)-(138), we obtain

$$\int_1^\infty \int_1^u (uv)^k e^{-uv} (\ln(uv)) \frac{1}{(u+v)^3} \, dv \, du = O\Big(k!(\log k)\, k^{-3/2}\Big) \ . \tag{139}$$

It follows from (131), (135), and (139) that

$$s_k = O\Big((\log k) \cdot k^{-3/2}\Big) \ . \tag{140}$$

We now need to derive an estimate for t_k. Note that

$$\begin{aligned} k!\, t_k &= O\left(\int_0^\infty \int_0^1 (uv)^k e^{-uv}\Big(\ln\frac{1}{v}\Big) \left\{\int_0^\infty x^2 e^{-(u+v)x} dx\right\} dv\, du\right) \\ &= O\left(\int_0^\infty \int_0^1 (uv)^k e^{-uv} \Big(\ln\frac{1}{v}\Big) \frac{1}{(u+v)^3} dv\, du\right) \\ &= O\left(\int_0^1 \Big(\ln\frac{1}{v}\Big) \left\{\int_0^\infty w^k e^{-w} \frac{1}{(\frac{w}{v}+v)^3} \frac{dw}{v}\right\} dv\right) \\ &= O\left(\int_0^1 v^2\Big(\ln\frac{1}{v}\Big) \left\{\int_0^\infty w^k e^{-w} \frac{dw}{(w+v^2)^3}\right\} dv\right) \\ &= O\left(\int_0^1 v^2\Big(\ln\frac{1}{v}\Big) \left\{\int_0^\infty w^{k-3} e^{-w} dw\right\} dv\right) \\ &= O\Big((k-3)!\Big) \ . \end{aligned}$$

Thus,

$$t_k = O(k^{-3}) \ . \tag{141}$$

It follows from (130), (140), and (141) that

$$\beta_{1,k} = O\Big((\log k) \cdot k^{-3/2}\Big) \ .$$

This completes the proof of item (c) in the lemma.

C2. Proof of Lemma 36.

We first prove the following identity: for all $k \geq 1$,

$$\beta_{0,k} = \frac{\sqrt{\pi}}{4} \int_0^1 \sqrt{1-x} \ x^k \, dx \ . \tag{142}$$

To prove (142), note that

$$\begin{aligned} \beta_{0,k} &= \frac{1}{k!} \int_0^\infty \int_0^\infty v^k x^2 e^{-vx-x^2} \left\{\int_0^\infty u^k e^{-u(v+x)} du\right\} dv\, dx \\ &= \frac{1}{k!} \int_0^\infty \int_0^\infty v^k x^2 e^{-vx-x^2} \frac{k!}{(v+x)^{k+1}} dv\, dx \ . \end{aligned}$$

Make a transformation of variables $x = \xi v$, and we obtain

$$\begin{aligned}
\beta_{0,k} &= \int_0^\infty \int_0^\infty \frac{\xi^2\, v^{k+2}}{(1+\xi)^{k+1}} \frac{1}{v^{k+1}}\, e^{-(\xi+\xi^2)v^2}\, v\, d\xi\, dv \\
&= \int_0^\infty \int_0^\infty \frac{\xi^2\, v^2}{(1+\xi)^{k+1}}\, e^{-(\xi+\xi^2)v^2}\, d\xi\, dv \\
&= \int_0^\infty \frac{\xi^2}{(1+\xi)^{k+1}} \left\{ \int_0^\infty v^2\, e^{-(\xi+\xi^2)v^2}\, dv \right\} d\xi \\
&= \int_0^\infty \frac{\xi^2}{(1+\xi)^{k+1}} \frac{\Gamma(3/2)}{2\xi^{3/2}\,(1+\xi)^{3/2}}\, d\xi \\
&= \frac{\sqrt{\pi}}{4} \int_0^\infty \frac{\sqrt{\xi}}{(1+\xi)^{k+5/2}}\, d\xi \ .
\end{aligned}$$

Make a transformation of variables $x = \frac{1}{1+\xi}$, and we obtain

$$\beta_{0,k} = \frac{\sqrt{\pi}}{4} \int_0^1 \sqrt{1-x}\, x^k\, dx \ .$$

This proves (142).

(a) Determining $<< H_k >>$.

Using (142), we have

$$\begin{aligned}
<< H_k >> &= \sum_{k\geq 1} H_k\, \beta_{0,k} \\
&= \frac{\sqrt{\pi}}{4} \sum_{k\geq 1} H_k \int_0^1 \sqrt{1-x}\, x^k\, dx \ . \qquad (143)
\end{aligned}$$

For any $0 < w < 1$, the following expansion is uniformly convergent for $|x| \leq w$:

$$\frac{1}{1-x} \ln \frac{1}{1-x} = \sum_{k\geq 1} H_k\, x^k \ .$$

It follows (see e.g. [A, Theorem 9.8]) that, for any $0 < w < 1$,

$$\begin{aligned}
\sum_{k\geq 1} H_k \int_0^w \sqrt{1-x}\ x^k\, dx &= \int_0^w \sqrt{1-x}\ \frac{1}{1-x} \ln \frac{1}{1-x}\, dx \\
&= \int_0^w \frac{1}{\sqrt{1-x}} \ln \frac{1}{1-x}\, dx \ . \qquad (144)
\end{aligned}$$

Note that $H_k \int_0^1 \sqrt{1-x}\, x^k\, dx = O\left((\log k)k^{-3/2}\right)$ by (142) and Lemma 35 (c). Thus the left-hand side of (144) is an infinite series of functions (of the variable w) that is uniformly convergent on the interval [0, 1]. We can interchange limit and summation (see e.g. [A, Theorem 9.7]) to obtain

$$\lim_{w\to 1-} \sum_{k\geq 1} H_k \int_0^w \sqrt{1-x}\, x^k\, dx = \sum_{k\geq 1} H_k \int_0^1 \sqrt{1-x}\, x^k\, dx \qquad (145)$$

It follows from (143)-(145) that

$$\begin{aligned}
<< H_k >> &= \frac{\sqrt{\pi}}{4} \sum_{k\geq 1} H_k \int_0^1 \sqrt{1-x}\, x^k\, dx \\
&= \frac{\sqrt{\pi}}{4} \lim_{w\to 1-} \left\{ \sum_{k\geq 1} H_k \int_0^w \sqrt{1-x}\, x^k\, dx \right\} \\
&= \frac{\sqrt{\pi}}{4} \lim_{w\to 1-} \int_0^w \frac{1}{\sqrt{1-x}} \ln \frac{1}{1-x}\, dx \\
&= \frac{\sqrt{\pi}}{4} \int_0^1 \frac{1}{\sqrt{1-x}} \ln \frac{1}{1-x}\, dx \\
&= -\frac{\sqrt{\pi}}{4} \int_0^1 \frac{1}{\sqrt{x}} \ln x\, dx \\
&= -\frac{\sqrt{\pi}}{4} \left\{ 2\sqrt{x} \ln x \Big|_{x=0}^{x=1} - 2\int_0^1 \sqrt{x}\, \frac{1}{x}\, dx \right\} \\
&= \sqrt{\pi}\ .
\end{aligned}$$

(b) Determining $<< H_k^{(2)} >>$.

Using (142), we have

$$<< H_k^{(2)} >> = \frac{\sqrt{\pi}}{4} \sum_{k\geq 1} H_k^{(2)} \int_0^1 \sqrt{1-x}\, x^k\, dx\ . \tag{146}$$

Define the following function $g(x)$ for $|x| < 1$,

$$g(x) = \frac{1}{1-x} \sum_{m\geq 1} \frac{1}{m^2}\, x^m\ . \tag{147}$$

For any $0 < w < 1$, the expansion (147) is uniformly convergent for $|x| \leq w$. It is elementary that, for any $0 \leq x < 1$,

$$\begin{aligned}
\sum_{k\geq 1} H_k^{(2)} x^k &= \sum_{k\geq 1} x^k \left(\sum_{1\leq j\leq k} \frac{1}{j^2} \right) \\
&= \sum_{m\geq 1} \left\{ \frac{1}{m^2} \sum_{k\geq m} x^k \right\} \\
&= \sum_{m\geq 1} \frac{1}{m^2} \frac{x^m}{1-x} \\
&= g(x)\ .
\end{aligned} \tag{148}$$

Thus, from (147) and (148), we have for all $|x| < 1$,

$$\sum_{k\geq 1} H_k^{(2)} x^k = \frac{1}{1-x} \sum_{m\geq 1} \frac{1}{m^2}\, x^m\ . \tag{149}$$

For any $0 < w < 1$, since (147) is uniformly convergent for $|x| \le w$, we can integrate term by term (see [A, Theorem 9.9]) to obtain

$$\begin{aligned}
\int_0^w \sqrt{1-x}\left(\sum_{k\ge1} H_k^{(2)} x^k\right) dx &= \int_0^w \frac{1}{\sqrt{1-x}}\left(\sum_{m\ge1}\frac{1}{m^2}\,x^m\right) dx \\
&= \sum_{m\ge1}\frac{1}{m^2}\int_0^w \frac{1}{\sqrt{1-x}}\,x^m\,dx \\
&= \sum_{m\ge1}\frac{1}{m^2}\left\{-2\sqrt{1-x}\,x^m\Big|_{x=0}^{x=w} + 2m\int_0^w \sqrt{1-x}\,x^{m-1}\,dx\right\} \\
&= -2\sqrt{1-w}\sum_{m\ge1}\frac{w^m}{m^2} + 2\sum_{m\ge1}\frac{1}{m}\int_0^w \sqrt{1-x}\,x^{m-1}\,dx\ . \qquad (150)
\end{aligned}$$

On the other hand, as $\sum_{k\ge1} H_k^{(2)}\sqrt{1-x}\ x^k$ is uniformly convergent for $|x| \le w$, we have

$$\int_0^w \sqrt{1-x}\left(\sum_{k\ge1} H_k^{(2)} x^k\right) dx = \sum_{k\ge1} H_k^{(2)}\int_0^w \sqrt{1-x}\ x^k\,dx\ . \qquad (151)$$

From (150) and (151), we have, for $0 < w < 1$

$$\sum_{k\ge1} H_k^{(2)}\int_0^w \sqrt{1-x}\ x^k\,dx = -2\sqrt{1-w}\sum_{m\ge1}\frac{w^m}{m^2} + 2\sum_{m\ge1}\frac{1}{m}\int_0^w \sqrt{1-x}\ x^{m-1}\,dx\ . \qquad (152)$$

Now, using similar reasoning as in the proof of (145), we obtain

$$\lim_{w\to1-}\left(\sum_{k\ge1} H_k^{(2)}\int_0^w \sqrt{1-x}\ x^k\,dx\right) = \sum_{k\ge1} H_k^{(2)}\int_0^1 \sqrt{1-x}\ x^k\,dx\ , \qquad (153)$$

and

$$\begin{aligned}
\lim_{w\to1-}\left(-2\sqrt{1-w}\sum_{m\ge1}\frac{w^m}{m^2} + 2\sum_{m\ge1}\frac{1}{m}\int_0^w \sqrt{1-x}\ x^{m-1}\,dx\right)& \\
= 2\sum_{m\ge1}\frac{1}{m}\int_0^1 \sqrt{1-x}\ x^{m-1}\,dx\ .& \qquad (154)
\end{aligned}$$

It follows from (146), (152)-(154) that

$$<< H_k^{(2)} >>= \frac{\sqrt{\pi}}{2}\sum_{m\ge1}\frac{1}{m}\int_0^1 \sqrt{1-x}\ x^{m-1}\,dx\ . \qquad (155)$$

By repeated partial integrations, we have

$$\begin{aligned}
\int_0^1 \sqrt{1-x}\ x^{m-1}\,dx &= \frac{(m-1)!}{\frac{3}{2}\cdot\frac{5}{2}\ \cdots\ \frac{2m+1}{2}} \\
&= \frac{4^m\,(m-1)!\,m!}{(2m+1)!}\ .
\end{aligned}$$

Thus,

$$<< H_k^{(2)} >> = \frac{\sqrt{\pi}}{2} \sum_{m \geq 1} \frac{4^m ((m-1)!)^2}{(2m+1)!} \ .$$

This proves item (b) in the lemma.

(c) Relating $((H_k))$ to $<< H_k^{(2)} >>$, $<< H_k >>$.

Let $f(u,k) = u^k \, e^{-u(v+x)}$. Then $f(u,k)$ satisfies the conditions in Apostol [A, Theorem 10.39], and hence $\int_0^\infty f(u,k)\, du$ exists, $\frac{\partial}{\partial k} \int_0^\infty f(u,k)\, du$ exists, and $\frac{\partial}{\partial k} \int_0^\infty f(u,k)\, du = \int_0^\infty \frac{\partial f(u,k)}{\partial k}\, du$. This means

$$\int_0^\infty (\ln u)\, u^k \, e^{-u(v+x)}\, dx = \frac{\partial}{\partial k} \left(\int_0^\infty u^k \, e^{-u(v+x)}\, du \right) \ . \tag{156}$$

We need another well-known identity (see [K2, Exercise 1.2.7.23]):

$$\frac{\Gamma'(k+1)}{\Gamma(k+1)} = H_k - \gamma \ , \tag{157}$$

where γ is the Euler's constant.

Now, using (156), we have, for all $k \geq 1$,

$$\begin{aligned}
\beta_{1,k} &= \frac{1}{k!} \int_0^\infty \int_0^\infty \int_0^\infty (\ln u)\, (uv)^k \, e^{-uv} \, x^2 \, e^{-x^2 - x(u+v)}\, dx\, du\, dv \\
&= \frac{1}{k!} \int_0^\infty \int_0^\infty v^k \, x^2 \, e^{-vx - x^2} \, \frac{\partial}{\partial k} \left[\int_0^\infty u^k \, e^{-u(v+x)}\, du \right] dv\, dx \\
&= \frac{1}{k!} \int_0^\infty \int_0^\infty v^k \, x^2 \, e^{-vx - x^2} \, \frac{\partial}{\partial k} \left(\frac{\Gamma(k+1)}{(v+x)^{k+1}} \right) dv\, dx \\
&= \frac{1}{k!} \int_0^\infty \int_0^\infty v^k \, x^2 \, e^{-x(v+x)} \left\{ \frac{\Gamma'(k+1)}{(v+x)^{k+1}} - \frac{\Gamma(k+1) \ln(v+x)}{(v+x)^{k+1}} \right\} dv\, dx \\
&= \frac{\Gamma'(k+1)}{\Gamma(k+1)} \int_0^\infty \int_0^\infty x^2 \, v^k \, e^{-x(v+x)} \frac{1}{(v+x)^{k+1}}\, dv\, dx \\
&\quad - \int_0^\infty \int_0^\infty x^2 \, v^k \, e^{-x(v+x)} \, \frac{\ln(v+x)}{(v+x)^{k+1}}\, dv\, dx \ .
\end{aligned} \tag{158}$$

These two last integrals can be shown to exist by standard arguments as used in the proof of Lemma 35 (a). (Proof omitted)

By (157), the expression in (158) is equal to

$$\begin{aligned}
&(H_k - \gamma) \int_0^\infty \int_0^\infty \int_0^\infty \psi_{0,k}(x,u,v)\, dx\, du\, dv \\
&- \int_0^\infty \int_0^\infty \int_0^\infty \psi_{0,k}(x,u,v) \ln(v+x)\, dx\, du\, dv \ .
\end{aligned}$$

Thus, we have

$$\begin{aligned}
((H_k)) &= << H_k^2 >> - \gamma \ << H_k >> \\
&- \sum_{k \geq 1} H_k \int_0^\infty \int_0^\infty \int_0^\infty \psi_{0,k}(x,u,v) \ln(v+x)\, dx\, du\, dv \ .
\end{aligned} \tag{159}$$

From (159) and the definition of $((H_k))$, we obtain

$$
\begin{aligned}
<< H_k^2 >> \quad - \quad 2((H_k)) &= \gamma << H_k >> \\
&\quad + \sum_{k\geq 1} H_k \int_0^\infty \int_0^\infty \int_0^\infty \psi_{0,k}(x,u,v)\ln(v+x)\,dx\,du\,dv \\
&\quad - \sum_{k\geq 1} H_k \int_0^\infty \int_0^\infty \int_0^\infty \psi_{0,k}(x,u,v)\ln v\,dx\,du\,dv \\
&= \gamma << H_k >> + C_0 \ , \qquad (160)
\end{aligned}
$$

where

$$
C_0 = \sum_{k\geq 1} H_k \int_0^\infty \int_0^\infty \int_0^\infty \psi_{0,k}(x,u,v)\ln\Big(1+\frac{x}{v}\Big)\,dx\,du\,dv \ .
$$

We now evaluate C_0, omitting the justification of standard manipulations such as the exchange of sum and integration, since we have done similar arguments earlier in the proofs of item (a) and item (b). Proceeding as in the proof of (142), we have

$$
\begin{aligned}
&\int_0^\infty \int_0^\infty \int_0^\infty \psi_{0,k}(x,u,v)\ln\Big(1+\frac{x}{v}\Big)\,dx\,du\,dv \\
&= \frac{\sqrt{\pi}}{4}\int_0^\infty \frac{\sqrt{\xi}}{(1+\xi)^{k+5/2}}\ln(1+\xi)\,d\xi \\
&= \frac{\sqrt{\pi}}{4}\int_0^1 \sqrt{1-x}\ x^k \ln\Big(\frac{1}{x}\Big)\,dx \ .
\end{aligned}
$$

Thus,

$$
\begin{aligned}
C_0 &= \frac{\sqrt{\pi}}{4}\int_0^1 \sqrt{1-x}\ \ln\Big(\frac{1}{x}\Big)\left(\sum_{k\geq 1} x^k H_k\right)dx \\
&= \frac{\sqrt{\pi}}{4}\int_0^1 \sqrt{1-x}\ \ln\Big(\frac{1}{x}\Big)\frac{1}{1-x}\ln\frac{1}{1-x}\,dx \\
&= \frac{\sqrt{\pi}}{4}\int_0^1 \frac{1}{\sqrt{1-x}}(\ln x)(\ln(1-x))\,dx \\
&= \frac{\sqrt{\pi}}{4}\int_0^1 \frac{1}{\sqrt{z}}(\ln z)(\ln(1-z))\,dz \\
&= -\frac{\sqrt{\pi}}{4}\sum_{m\geq 1}\frac{1}{m}\int_0^1 z^{m-1/2}\ln z\,dz \\
&= -\frac{\sqrt{\pi}}{4}\sum_{m\geq 1}\frac{1}{m}\left\{\frac{1}{m+1/2}z^{m+1/2}\ln z\,\Big|_{z=0}^{z=1} - \frac{1}{m+1/2}\int_0^1 z^{m-1/2}\,dz\right\} \\
&= -\frac{\sqrt{\pi}}{4}\sum_{m\geq 1}\frac{1}{m}\left\{-\frac{1}{(m+1/2)^2}\right\} \\
&= \frac{\sqrt{\pi}}{4}\sum_{m\geq 1}\frac{1}{m}\frac{4}{(2m+1)^2} \ . \qquad (161)
\end{aligned}
$$

From (160) and (161), we have then

$$<< H_k^2 >> - 2((H_k)) = \gamma << H_k >> + \frac{\sqrt{\pi}}{4} \sum_{m \geq 1} \frac{1}{m} \frac{4}{(2m+1)^2} \ .$$

This completes the proof of item (c) in Lemma 36.

References

[A] T. M. Apostol, *Mathematical Analysis*, second edition, Addison-Wesley, Reading, Massachusetts, 1974.

[FS] P. Flajolet and R. Sedgewick, *Average-Case Analysis of Algorithms*, Princeton, 1989, to appear.

[FV] P. Flajolet and J. S. Vitter, "Average-case analysis of algorithms and data structures," in *Handbook of Theoretical Computer Science*, edited by J. van Leeuwen, North-Holland, Amsterdam, 1989, to appear.

[GK] D. H. Greene and D. E. Knuth, *Mathematics for the Analysis of Algorithms*, Birkhauser, Boston, 1981.

[K1] D. E. Knuth, "Mathematical Analysis of Algorithms," in *Information Processing 71* (Proceedings of IFIP Congress 1971), 19-27, North-Holland, Amsterdam, 1972.

[K2] D. E. Knuth, *The Art of Computer Programming, Vol. 1: Fundamental Algorithms*, second edition, Addison-Wesley, Reading, Massachusetts, 1973.

[K3] D. E. Knuth, *The Art of Computer Programming, Vol. 3: Sorting and Searching*, Addison-Wesley, Reading, Massachusetts, 1973.

[R] A. Rényi, *Foundations of Probability*, Holden-Day, San Francisco, California, 1970.

[S] R. Sedgewick, "The analysis of Quicksort programs," *Acta Informatica* **7** (1977), 327-355.

[Y] A. C. Yao, "An analysis of (h, k, 1)-Shellsort," *Journal of Algorithms* **1** (1980), 14-50.