PROBABILISTIC AND COMBINATORIAL ASPECTS OF THE CARD-CYCLIC TO RANDOM INSERTION SHUFFLE

ROSS G. PINSKY

Abstract. Consider a permutation $\sigma \in S_n$ as a deck of cards numbered from 1 to n and laid out in a row, where σ_j denotes the number of the card that is in the j-th position from the left. We study some probabilistic and combinatorial aspects of the shuffle on S_n defined by removing and then randomly reinserting each of the n cards once, with the removal and reinsertion being performed according to the original left to right order of the cards. The novelty here in this nonstandard shuffle is that every card is removed and reinserted exactly once. The bias that remains turns out to be quite strong and possesses some surprising features.

1. Introduction and Statement of Results

Let S_n denote the symmetric group of permutations of $[n] \equiv \{1, \cdots, n\}$. Our convention will be to view a permutation $\sigma \in S_n$ as a deck of cards numbered from 1 to n and laid out in a row, where σ_j denotes the number of the card that is in the j-th position from the left. In this paper, we analyze the bias in the following "shuffle" on n cards: remove and then randomly reinsert each of the n cards exactly once, the removal and reinsertion being performed according to the *original* left to right order of the cards. The novelty here in this nonstandard shuffle is that *every card is removed and reinserted exactly once*, unlike in any of the shuffles one encounters in the literature. The point is to see how much bias remains when one knows that every card has been removed and reinserted.

We dub this shuffle the *card-cyclic to random insertion shuffle.* The reason for this terminology along with the original motivation that led to the study

2000 *Mathematics Subject Classification.* 60C05, 05A05, 05A15.

Key words and phrases. random shuffle, random permutation, total variation norm.

of this shuffle will be explained at the end of this section. However, we feel that the results are of independent interest regardless of that motivation.

We let $p_n(\sigma,\tau)$ denote the probability that the deck ends up in the state $\tau \in S_n$, given that it began in state $\sigma \in S_n$. Of course, since the shuffle is transitive, it suffices to look at $p_n(\mathrm{id},\cdot)$, where id is the identity element, corresponding to the cards being in increasing order from left to right. Note that if $n \ge 3$, the distribution after one such shuffle cannot be exactly uniform because there are n^n equally probable ways to implement the shuffle, but there are $n!$ possible states of the deck, and $n! \nmid n^n$. Of course this doesn't rule out asymptotic uniformity, but in fact we shall see that the card-cyclic to random insertion shuffle is far from uniform.

We begin with the behavior of the distribution of the card in the first position and of the card in the last position. The bias with regard to the first position turns out to be quite strong.

Theorem 1. *Under $p_n(id,\cdot)$, the random variable σ_1, denoting the number of the card in the first position, has the following behavior:*

(1.1)
$$p_n(id,\{\sigma_1=j\}) = \frac{1}{n}e^{\frac{j}{n}-1}\big(1+O(\frac{1}{n})\big) + \frac{1}{e\sqrt{n}}\psi(\frac{j}{\sqrt{n}})\big(1+O(n^{-0.2})\big) + O(e^{-n^{0.1}}),$$
uniformly in j as $n\to\infty$, where $\psi(t) \equiv \int_t^\infty e^{-\frac{1}{2}x^2}dx.$

In particular then, the following limits hold.

i.

$$\lim_{n\to\infty} np_n(id,\{\sigma_1=b_nn\}) = e^{b-1},\ \text{if}\ \lim_{n\to\infty} b_n = b\in(0,1],$$
$$\text{or if}\ \lim_{n\to\infty} b_n = b = 0\ \text{and}\ \lim_{n\to\infty} n^{\frac{1}{2}}b_n = \infty. \tag{1.2}$$

Thus, defining the probability measure ν_n^F on $[0,1]$ by

$$\nu_n^F(A) = p_n(id,\{\sigma_1\in nA\}), A\subset[0,1],$$

one has

$$w-lim_{n\to\infty}\nu_n^F(dx) = e^{-1}\delta_0(x) + e^{x-1}dx.$$

ii.

$$\lim_{n\to\infty} n^{\frac{1}{2}} p_n(id, \{\sigma_1 = d_n n^{\frac{1}{2}}\}) = e^{-1}\int_d^\infty e^{-\frac{y^2}{2}}dy, \tag{1.3}$$
$$\text{if } \lim_{n\to\infty} d_n = d \in [0,\infty).$$

Thus, defining the probability measure μ_n^F *on* $[0,\infty)$ *by*

$$\mu_n^F(A) = p_n(id, \{\sigma_1 \in n^{\frac{1}{2}}A\}), A \subset [0,\infty),$$

one has

$$v - \lim_{n\to\infty} \mu_n^F(dx) = e^{-1}\Big(\int_x^\infty e^{-\frac{y^2}{2}}dy\Big)dx,$$

the total mass of the measure on the right hand side above being e^{-1}*.*

Remark. From Theorem 1, it follows that *the most likely numbers for the first position lie "right next to" the least likely numbers.* More precisely, the following facts follow from Theorem 1:

1. (Most likely asymptotic numbers for first position) Let $\{\gamma_n\}_{n=1}^\infty$ denote a sequence satisfying $1 \le \gamma_n \le n$, for each n. Then

$$\sup_{\{\gamma_n\}_{n=1}^\infty} \limsup_{n\to\infty} n^{\frac{1}{2}} p_n(\mathrm{id}, \{\sigma_1 = \gamma_n\}) = \frac{\sqrt{2\pi}}{2e}.$$

In particular, the supremum is attained for sequences $\{\gamma_n\}_{n=1}^\infty$ satisfying $\gamma_n = o(n^{\frac{1}{2}})$, as $n \to \infty$

2. (Least likely asymptotic numbers for first position) Let $\{\gamma_n\}_{n=1}^\infty$ denote a sequence satisfying $1 \le \gamma_n \le n$, for each n. Then

$$\inf_{\{\gamma_n\}_{n=1}^\infty} \liminf_{n\to\infty} np_n(\mathrm{id}, \{\sigma_1 = \gamma_n\}) = e^{-1}.$$

In particular, the infimum is attained for sequences $\{\gamma_n\}_{n=1}^\infty$ satisfying $\gamma_n = o(n)$ and $\sqrt{n} = o(\gamma_n)$, as $n \to \infty$.

The bias with regard to the last position is considerably tamer than the bias with regard to the first position.

Theorem 2. *Under* $p_n(id,\cdot)$*, the random variable* σ_n*, denoting the number of the card in the last position, has the following behavior.*

i.

$$\lim_{n\to\infty} np_n(id, \{\sigma_n = b_n n\}) = \frac{e^b}{e-1}, \text{ if } \lim_{n\to\infty} b_n = b \in [0,1). \tag{1.4}$$

In particular then, defining the probability measure ν_n^L *on* $[0,1]$ *by*

$$\nu_n^L(A) = p_n(id, \{\sigma_n \in nA\}), A \subset [0,1],$$

one has

$$w - lim_{n\to\infty} \nu_n^L(dx) = \frac{e^x}{e-1} dx.$$

ii.

(1.5)

$$\lim_{n\to\infty} np_n(id, \{\sigma_n = b_n n\}) = \frac{e}{e-1}, \ \textit{if} \ \lim_{n\to\infty} b_n = 1 \ \textit{and} \ \lim_{n\to\infty}(n - b_n n) = \infty.$$

iii.

$$\lim_{n\to\infty} np_n(id, \{\sigma_n = n - l\}) = \frac{e - e^{-l}}{e-1}, \ l = 0, 1, \cdots. \tag{1.6}$$

Remark. The following facts follow from Theorem 2.

1. (Most likely asymptotic numbers for last position) Let $\{\gamma_n\}_{n=1}^\infty$ denote a sequence satisfying $1 \le \gamma_n \le n$, for each n. Then

$$\sup_{\{\gamma_n\}_{n=1}^\infty} \limsup_{n\to\infty} np_n(\mathrm{id}, \{\sigma_n = \gamma_n\}) = \frac{e}{e-1}.$$

In particular, the supremum is attained for sequences $\{\gamma_n\}_{n=1}^\infty$ satisfying $\lim_{n\to\infty} \frac{\gamma_n}{n} = 1$ and $\lim_{n\to\infty}(n - \gamma_n) = \infty$.

2. (Least likely asymptotic numbers for last position) Let $\{\gamma_n\}_{n=1}^\infty$ denote a sequence satisfying $1 \le \gamma_n \le n$, for each n. Then

$$\inf_{\{\gamma_n\}_{n=1}^\infty} \liminf_{n\to\infty} np_n(\mathrm{id}, \{\sigma_n = \gamma_n\}) = \frac{1}{e-1}.$$

In particular, the supremum is attained for sequences $\{\gamma_n\}_{n=1}^\infty$ satisfying $\gamma_n = o(n)$.

Theorem 1 showed that the cards with numbers on the order $n^{\frac{1}{2}}$ are more likely to occupy the first position than cards with larger numbers. In fact, more generally, cards with numbers on the order $n^{\frac{1}{2}}$ are more likely to occupy any position at the beginning of the deck than are cards with larger numbers. We can quantify this and use it to prove that the total variation norm between the card-cyclic to random insertion shuffle measure and the uniform measure converges to 1 as $n \to \infty$. Recall that the total variation norm between two probability measures μ and ν on S_n is defined by

$$||\mu - \nu||_{\mathrm{TV}} = \sup_{A \subset S_n} (\mu(A) - \nu(A)) = \frac{1}{2} \sum_{\sigma \in S_n} |\mu(\sigma) - \nu(\sigma)|.$$

Theorem 3. *Let*

$$A^{(n)}_{M,L} = \{\sigma \in S_n : \sigma_j \le M n^{\frac{1}{2}},\ \textit{for some } j \le L\}$$

be the event that a card with a number less than or equal to $Mn^{\frac{1}{2}}$ *appears in one of the first* L *positions. Then*

$$\lim_{C \to \infty} \lim_{M \to \infty} \lim_{n \to \infty} p_n(id, A^{(n)}_{M,CM^2}) = 1. \tag{1.7}$$

In particular then,

$$\lim_{n \to \infty} ||p_n(id, \cdot) - U_n||_{TV} = 1. \tag{1.8}$$

The first two theorems dealt with the distribution of the *number of the card* in special positions—namely, the first and the last positions. We now consider the distribution of the *position of the card* with a general number.

Theorem 4. *Under* $p_n(id, \cdot)$*, the random variable* $\sigma^{-1}_{b_n n}$*, denoting the position of card number* $b_n n$*, has the following behavior. Assume that* $\lim_{n \to \infty} b_n = b \in [0,1]$*. Then the weak limit of the distribution of* $\frac{1}{n}\sigma^{-1}_{b_n n}$ *exists. Its distribution function*

$$F_b(x) \equiv \lim_{n \to \infty} p_n(id, \{\sigma^{-1}_{b_n n} \le xn\}),\ x \in [0,1],$$

is given as follows. Define $G_b : [0,1] \to [0,1]$ *by*

$$G_b(y) = \begin{cases} ye^{1-b}, & 0 \le y \le 1 - (1-b)e^b; \\ e^{(1-y)e^{-b}} - (1-y)e^{1-b}, & 1 - (1-b)e^b \le y \le 1. \end{cases}$$

Then $F_b = G_b^{-1}$.

We have the following corollary. Part (iii) of the corollary follows from part (i) of Corollary 5 below. The rest of the parts are a pedestrian calculus exercise.

Corollary 1. *Let f_b denote the density of the distribution function F_b, that is, the density function for the limiting rescaled position of a card with a number around bn. Let $x_b = e^{1-b} - (1-b)e$, $0 \le b \le 1$, and let b_x, $0 \le x \le 1$, denote its inverse. Note that $b_1 = 1$. Then $f_1 \equiv 1$, and for $b \in [0,1)$,*
i. $f_b(x) = e^{b-1}$, $0 \le x < x_b$;
ii. $f_b(x_b^+) = \frac{e^{b-1}}{1-e^{-b}}$;
iii. $f_b(x) = \frac{e^{b+b_x-1}}{e^{b_x}-1}$, $x_b < x \le 1$.

Remark. Note that f_b is constant on $[0, x_b)$, where it attains its minimum. It is decreasing on $(x_b, 1]$ and its supremum is $f_b(x_b^+)$. The corollary shows that for a card with a number around bn, with $b \in (0,1)$, the most likely positions in which it will end up are those just to the right of $nx_b = n(e^{1-b} - (1-b)e)$, and the least likely positions are all of those less than nx_b. In particular, *the most likely positions for a card with a number around bn lie "right next to" the least likely positions.* See figure 1. Note also that $f_0(0) = \infty$, which means that for all b and d, the probability of a card with a number around bn ending up in a position around dn is the greatest for $b = d = 0$. (This connects up with Theorem 1.) The probability measures corresponding to the densities f_b are weakly continuous with respect to $b \in [0,1]$. For each $b \in (0,1)$, the density f_b has a discontinuity, however considered as cadlag functions, the densities f_b vary continuously in the Skorohod topology for $b \in (0,1)$. This continuity does not extend to $b = 0$, where $f_0(0) = \infty$, or to $b = 1$, where $f_1 \equiv 1$ but $\lim_{b\to 1} \sup_{x\in[0,1]} f_b(x) = \frac{e}{e-1}$.

Let $E^{p_n(\mathrm{id},\cdot)}$ denote the expectation corresponding to the card-cyclic to random insertion shuffle starting from id, so that $E^{p_n(\mathrm{id},\cdot)}\sigma^{-1}_{b_n n}$ is the expected position for card number $b_n n$ at the end of the shuffle. It follows from the theorem that if $\lim_{n\to\infty} b_n = b$, then $E(b) \equiv \lim_{n\to\infty} \frac{1}{n} E^{p_n(\mathrm{id},\cdot)}\sigma^{-1}_{b_n n}$ exists and is given by $\int_0^1 (1 - F_b(x))dx$. Making a substitution and integrating by parts shows that this integral is equal to $\int_0^1 G_b(y)dy$. Computing this integral then gives the following corollary.

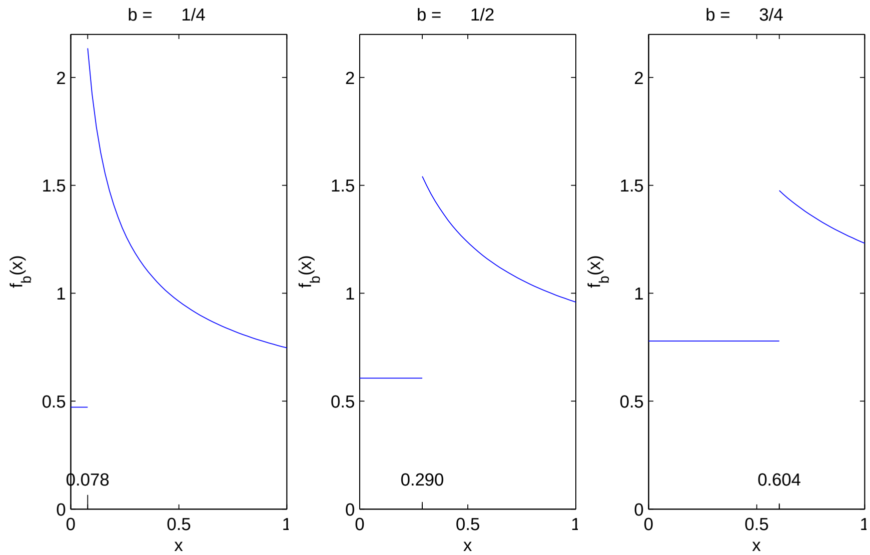

FIGURE 1. Density for limiting rescaled position of a card with a number around bn.

Corollary 2. *Let $E(b) \equiv \lim_{n\to\infty} \frac{1}{n} E^{p_n(id,\cdot)} \sigma^{-1}_{b_n n}$, where $\lim_{n\to\infty} b_n = b$, denote the rescaled limiting expected position for a card with a number around bn. Then*

$$E(b) = eb + \frac{1}{2}e^{1-b} - e^b.$$

The function $E(b)$ has the following properties:

i. $E(0) = \frac{1}{2}e - 1 \approx .359$*;*

ii. $E(1) = \frac{1}{2}$*;*

iii. $E(\cdot)$ *increases for* $b \in [0, b^*]$ *and decreases for* $b \in [b^*, 1]$*, where* $b^* \approx .722$ *is the solution to* $e - e^b - \frac{1}{2}e^{1-b} = 0$*. The maximum value of* $E(\cdot)$ *is* $E(b^*) \approx .564$*;*

iv. $E(b) \geq b$*, for* $b \in [0, \bar{b}]$ *and* $E(b) \leq b$ *for* $b \in [\bar{b}, 1]$*, where* $\bar{b} \approx .545$*.*

v. $\int_0^1 E(b)db = \frac{1}{2}$*.*

Remark. In particular, a card starting out very near the left end of the deck will end up on the average around 35.9 percent of the way through the deck, while a card starting out anywhere else will end up on the average further to the right than this. A card starting out around 72.2 percent of the way through the deck will end up on the average around 56.4 percent of the way through the deck, while a card starting out anywhere else will end up on the

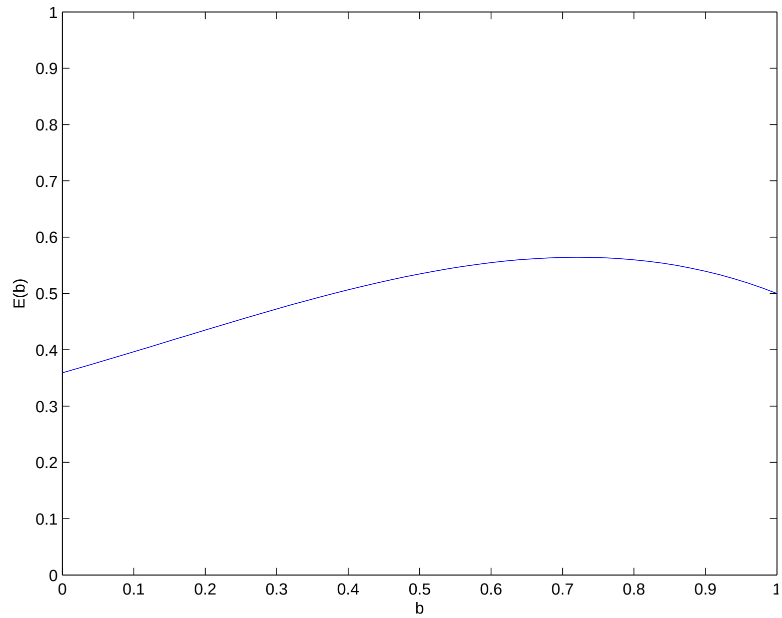

FIGURE 2. Limiting rescaled expected position of a card with a number around bn.

average further to the left than this. A card in the first 54.5 percent of the deck will end up on the average further to the right than where it started, while a card in the last 45.5 percent of the deck will end up on the average further to the left than where it started. See figure 2. But of course, as (v) indicates and as is clear from considerations of symmetry, the average ending position of the average card must be the 50th percentile.

The following corollary shows that the random positions of a finite number of cards are asymptotically independent. The result follows easily from the proof of Theorem 4, as will be shown after the proof of that theorem.

Corollary 3. *For $m \ge 1$, let $1 \le b_{1n}n < b_{2n}n < \cdots < b_{mn}n \le n$ satisfy $\lim_{n\to\infty} b_{jn} = b_j \in [0,1]$; so $0 \le b_1 \le b_2 \le \cdots \le b_m \le 1$. Then under $p_n(id,\cdot)$, the distribution of the random vector $\frac{1}{n}(\sigma^{-1}_{b_{1n}n}, \sigma^{-1}_{b_{2n}n}, \cdots, \sigma^{-1}_{b_{mn}n})$ converges to the m-dimensional product distribution with density $\prod_{j=1}^m f_{b_j}(x_j)$, where $x = (x_1, \cdots, x_m)$.*

We can use the above corollary to say something about the probability of inversions. For $i < j$, if card number j appears to the left of card number i

in a permutation σ, then we say that the pair of cards with numbers i and j form an *inversion* for the permutation σ. This concept is described more fully below, two paragraphs above Lemma 1. For $m = 2$ in Corollary 3, let $(\Sigma^{-1}_{1;b_1}, \Sigma^{-1}_{2;b_2})$ denote a random vector distributed according to the density $f_{b_1}(x_1)f_{b_2}(x_2)$. We will prove the following result.

Corollary 4. *i. Let $\hat{b} \approx .768$ be the root of the equation $(1-b)e^b - \frac{1}{2} = 0$. Then*

$$P(\Sigma^{-1}_{1;b_1} < \Sigma^{-1}_{2;b_2}) > \frac{1}{2}, \text{ for } b_1 < b_2 < \hat{b} \text{ and } b_2 \text{ sufficiently close to } b_1;$$
$$P(\Sigma^{-1}_{1;b_1} < \Sigma^{-1}_{2;b_2}) < \frac{1}{2}, \text{ for } \hat{b} < b_1 < b_2 \text{ and } b_2 \text{ sufficiently close to } b_1;$$

ii. Let $\tilde{b} \approx .380$ be the unique root of the equation $E(b) = \frac{1}{2}$, for $b \in [0, 1)$, where $E(b)$ is as in Corollary 2. Then

$$P(\Sigma^{-1}_{1;b} < \Sigma^{-1}_{2;1}) > \frac{1}{2}, \text{ for } b \in [0, \tilde{b});$$
$$P(\Sigma^{-1}_{1;b} < \Sigma^{-1}_{2;1}) < \frac{1}{2}, \text{ for } b \in (\tilde{b}, 1).$$

Remark. The first part of the corollary indicates that for large n, if one takes a card with a number around $b_1 n$ and a card with a number around $b_2 n$, with $b_2 > b_1$ and sufficiently close to b_1, then under $p_n(\mathrm{id}, \cdot)$, the probability that these cards form an inversion is less than $\frac{1}{2}$ if $b_1 < \hat{b} \approx .768$ and greater than $\frac{1}{2}$ if $b_1 > \hat{b} \approx .768$. (We suspect that the restriction that b_2 be close to b_1 is unnecessary for the above result.) The second part of the corollary indicates that for large n, if one takes a card with a number around bn, $b \in (0, 1)$, and a card with a number around n (that is, a card from the very end of the deck), then under $p_n(\mathrm{id}, \cdot)$, the probability that these cards form an inversion is less than $\frac{1}{2}$ if $b < \tilde{b}$ and greater than $\frac{1}{2}$ if $b > \tilde{b}$. Furthermore, the point $b = \tilde{b}$ where the probability is equal to $\frac{1}{2}$ is exactly the point b where the limiting average rescaled position $E(b)$ is equal to $\frac{1}{2}$. Despite the above corollary, the measure $p_n(\mathrm{id}, \cdot)$ favors permutations that do not have a lot of inversions, in a sense made precise in Corollary 6 below. See also, the remark after that corollary.

The results in Theorems 1 and 2 are local limit theorems. If we had such a local result in Theorem 4; namely $\lim_{n\to\infty} np_n(\mathrm{id}, \{\sigma^{-1}_{b_n n} = x_n n\}) = f_b(x)$, whenever $\lim_{n\to\infty} b_n = b$ and $\lim_{n\to\infty} x_n = x$ with $x \neq x_b$, rather than only

$$\lim_{n\to\infty} p_n(\mathrm{id}, \{\sigma^{-1}_{b_n n} \le xn\}) = F_b(x), \tag{1.9}$$

then it would follow by a compactness argument that $\lim_{n\to\infty} p_n(\mathrm{id}, \{\sigma_{x_n n} \le b_n n\}) = \int_0^b f_t(x)dt$ whenever $\lim_{n\to\infty} x_n = x$, $\lim_{n\to\infty} b_n = b$ and at least one of x and b is different from 0. Unfortunately, we don't see how to prove this rigorously just from (1.9), nor do we see how to prove directly that $\lim_{n\to\infty} p_n(\mathrm{id}, \{\sigma_{x_n n} \le bn\})$ exists, although it is intuitively obvious that it does. And if it does exist, then it is easy to show that the corresponding density must be $h_x(b) \equiv f_b(x)$, except at $x = 0$ and at points of discontinuity of $f_b(x)$. We prove the following corollary concerning $h_x(b)$, the limiting rescaled expected card number occupying a position around xn. The proof of part (i) of the corollary gives a proof of part (iii) of Corollary 1.

Corollary 5. *The density function $h_x(b)$, the limiting rescaled card number occupying a position around xn, has the following behavior.*

For $x = 0$, one has $h_0(b) = e^{b-1}, 0 < b < 1$. This is a sub-probability density with total mass $1 - e^{-1}$. In addition there is a δ-mass of size e^{-1} at $b = 0$.

For $x = 1$, one has $h_1(b) = \frac{e^b}{e-1}, 0 \le b \le 1$.

Let b_x, $0 < x < 1$, denote the inverse of the function $x_b = e^{1-b} - (1-b)e$, $0 < b < 1$. For $0 < x < 1$, one has

i. $h_x(b) = \frac{e^{b+b_x-1}}{e^{b_x}-1}$, $0 \le b < b_x$;

ii. $h_x(b) = e^{b-1}$, $b_x < b \le 1$.

Remark. The fact that at $x = 0$ there is a δ mass at 0 of size e^{-1} connects up with Theorem 1. The corollary shows that the most likely numbers to find in a position around xn, $0 < x < 1$, are numbers slightly smaller than nb_x. If $e^{b_x} < 2$, or equivalently, $x < \frac{1}{2}e - (1 - \ln 2)e \approx .525$, then the least likely numbers to find in a position around xn are numbers slightly larger than nb_x; if $x > \frac{1}{2}e - (1 - \ln 2)e$, then the least likely numbers to find in a position around xn are numbers on order $o(n)$. *In particular, for all $x \in [0, 1]$, the most likely numbers for a position around xn are "right next to" numbers that are much less likely to be in such a position, and*

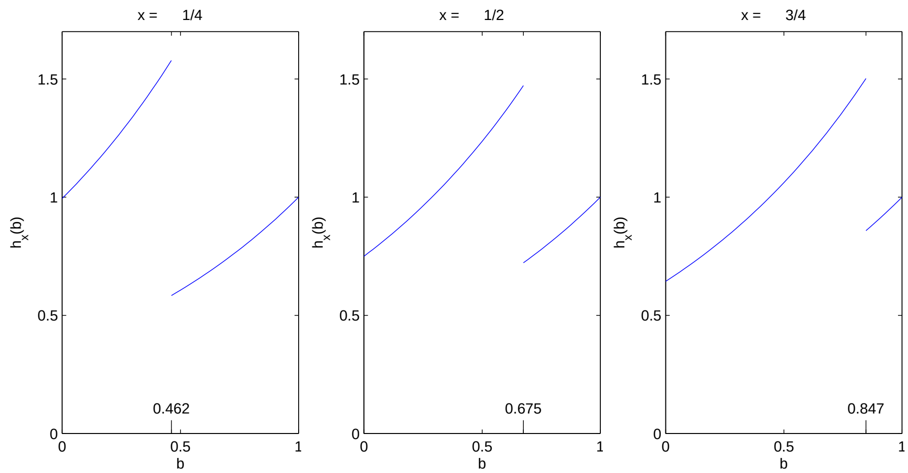

FIGURE 3. Density for limiting rescaled card number occupying a position around xn.

if $x < \frac{1}{2}e - (1 - \ln 2)e \approx .525$, *then these latter numbers are the least likely ones to be in such a position.* See figure 3. The probability measures corresponding to the densities h_x are weakly continuous with respect to $x \in (0, 1]$, and the densities h_x, considered as cadlag functions with the Skorohod topology, vary continuously for $x \in (0, 1)$.

We now turn to the study of the entire distribution $p_n(\mathrm{id}, \cdot)$. We need to introduce some additional concepts and notation. Fix a positive integer n. Let $l = (l_1, \cdots, l_{n-1})$ be an $(n-1)$-vector of positive integers satisfying $i \le l_i \le n - 1$. Consider the collection of all integer-valued paths $\{Y_i\}_{i=1}^n$ satisfying $1 \le Y_1 \le Y_2 \le \cdots \le Y_n = n$, with the strict inequality $Y_{i+1} > Y_i$ holding if $Y_i \le l_i$. Note that one always has $Y_i \ge i$, for all $i = 1, \cdots, n$. Call such paths *nondecreasing* l*-paths of length* n. Denote the number of such paths by $N_n(l)$. Note that $N_n(l)$ is strictly decreasing in each of its $n - 1$ variables.

Recall that for $\sigma \in S_n$ and $i, j \in [n]$ with $i < j$, the pair (i, j) is called an *inversion* for σ if $\sigma_j < \sigma_i$. According to our convention, (i, j) is an inversion for σ if the card in *position* i has a higher number than the card in *position* j. Thus, (i, j) is an inversion for the inverse permutation σ^{-1} if the card *numbered* i appears to the right of the card *numbered* j in the permutation

σ. In this case, as we have already noted before Corollary 4, we also say that the cards with numbers i and j form an inversion for σ. For $2 \le j \le n-1$ and $\sigma \in S_n$, let

$$I_j(\sigma) = \sum_{k=1}^{j-1} 1_{\sigma_k^{-1} > \sigma_j^{-1}} = \# \text{ of inversions in } \sigma$$

$$\text{involving the card numbered } \ j \ \text{ and a card numbered less than } j.$$

For convenience, we also define $I_1(\sigma) = 0$. Define $l(\sigma) = (l_1(\sigma), \cdots, l_{n-1}(\sigma))$ by

$$l_j(\sigma) = j + I_{n-j}(\sigma), \ j = 1, \cdots, n-1.$$

Note that $j \le l_j(\sigma) \le n-1, \ j = 1, \cdots, n-1$.

Lemma 1. *For each $l = (l_1, \cdots, l_{n-1})$ satisfying $j \le l_j \le n-1$, for $j = 1, \cdots, n-1$, there exist exactly n permutations $\sigma \in S_n$ satisfying $l(\sigma) = l$.*

Proof. Note that $l(\sigma)$ does not depend on σ_n^{-1}, the position in σ of the card numbered n, with the relative positions of cards $1, 2, \cdots, n-1$ held fixed. It is easy to see that any $\sigma \in S_n$ is uniquely determined by the value of σ_n^{-1} and by the condition $l(\sigma) = l$, where $l = (l_1, \cdots, l_{n-1})$ is as in the statement of the lemma. □

Theorem 5. *Let $\sigma \in S_n$. One has*

$$p_n(id, \sigma) = \frac{N_n(l(\sigma))}{n^n},$$

where $N_n(l)$ denotes the number of nondecreasing l-paths of length n.

Theorem 5 gives a qualitative picture of the nature of the bias in the $p_n(\mathrm{id}, \cdot)$-shuffle. Indeed, using the strict monotonicity of $N(l)$ and the definition of $l(\sigma)$, the following corollary is immediate from Theorem 5.

Corollary 6. *i. $p_n(id, \sigma)$ does not depend on σ_n^{-1}, the position in σ of card number n, with the relative positions of cards $1, 2 \cdots, n-1$ held fixed;*
ii. Let $\sigma', \sigma'' \in S_n$. If $I_j(\sigma') \le I_j(\sigma'')$, for all $j \in \{2, \cdots, n-1\}$, then

$$p_n(id, \sigma') \ge p_n(id, \sigma''),$$

with strict inequality holding if $I_j(\sigma') < I_j(\sigma'')$, for some $j \in \{2, \cdots, n-1\}$.

Remark. Of course, we don't need the theorem to get part (i) of the corollary. From the definition of the shuffle, it is clear that the distribution of card number n is uniform. Part (ii) shows in particular that among cards numbered from 1 to $n-1$, if every such pair of cards that forms an inversion for σ' also forms an inversion for σ'', then $p_n(\mathrm{id},\sigma') \geq p_n(\mathrm{id},\sigma'')$. Thus, in the above sense, the more a permutation preserves the order defined by id, but ignoring card number n, the more it is favored by $p_n(\mathrm{id},\cdot)$. *We have qualified the above sentence with the words "in the above sense," because Corollary 4 shows that if n is large and $b_2 > b_1 > \hat{b} \approx .768$, with b_2 close to b_1, then $p_n(id,\cdot)$ assigns a probability greater than $\frac{1}{2}$ to those permutations for which card number $[b_1 n]$ and card number $[b_2 n]$ form an inversion!*

It seems quite difficult to estimate $N_n(l)$ for general l. However, the maximum and minimum over l can be calculated explicitly.

Theorem 6. *One has*

$$2^{n-1} \leq N_n(l) \leq \frac{1}{n+1}\binom{2n}{n}, \tag{1.10}$$

for all $l = (l_1, \cdots, l_{n-1})$, with $j \leq l_j \leq n-1$, for $j = 1, \cdots, n-1$. The left hand inequality above is an equality if and only if $l_j = n-1$, for all $j = 1, \cdots, n-1$, and the right hand inequality above is an equality if and only if $l_j = j$, for all $j = 1, \cdots, n-1$.

Remark. Note that the right hand term in (1.10) is equal to C_n, the nth Catalan number.

The following corollary is immediate from Theorems 5 and 6.

Corollary 7. *One has*

$$\frac{2^{n-1}}{n^n} \leq p_n(id,\sigma) \leq \frac{\binom{2n}{n}}{(n+1)n^n}. \tag{1.11}$$

The right hand inequality above is an equality if and only if σ possesses the increasing subsequence $1, \cdots, n-1$, and the left hand inequality is an equality if and only if σ possesses the decreasing subsequence $n-1, \cdots, 1$.

Note that the left hand side of (1.11) is $\frac{1}{2}\frac{2^n}{n^n}$ and the right hand side of (1.11) behaves asymptotically as $n \to \infty$ like $\frac{1}{\sqrt{\pi} n^{\frac{3}{2}}}\frac{4^n}{n^n}$, while the uniform probability measure $U_n(\sigma) = \frac{1}{n!}$ behaves asymptotically as $n \to \infty$ like $\frac{1}{\sqrt{2\pi n}}\frac{e^n}{n^n}$. Thus, we have the following tight uniform bounds over $\sigma \in S_n$:

$$(1+o(1))(\frac{\pi n}{2})^{\frac{1}{2}}(\frac{2}{e})^n \le \frac{p_n(\mathrm{id},\sigma)}{U_n(\sigma)} \le (1+o(1))\frac{\sqrt{2}}{n}(\frac{4}{e})^n, \text{ as } n \to \infty.$$

In particular, the *separation distance* between U_n and $p_n(\mathrm{id},\cdot)$ approaches 1 exponentially fast as $n \to \infty$. (Recall that the separation distance s is defined by $s(p_n(\mathrm{id},\cdot), U_n) = \max_{\sigma \in S_n}(1 - \frac{p_n(\mathrm{id},\sigma)}{U_n(\sigma)})$.)

Consider now the random walk with increment distribution given by $p_n(\cdot,\cdot)$.

Corollary 8. *The random walk on S_n with increment transition measure $p_n(\cdot,\cdot)$ is not reversible.*

Proof. From the formula in Theorem 5, it is easy to see that the equality $p_n(\mathrm{id},\sigma) = p_n(\mathrm{id},\sigma^{-1})$ does not hold for all $\sigma \in S_n$. □

In a prior preprint version of this paper, we posed the question: how long does it take for this random walk to mix? That is, letting $(p_n)^m(\mathrm{id},\cdot)$ denote the m-fold convolution of $p_n(\mathrm{id},\cdot)$, which is the distribution of the random walk at time m given that it started from id, how large must $\{m_n\}_{n=1}^\infty$ be so that $\lim_{n\to\infty} ||U_n - (p_n)^{m_n}(\mathrm{id},\cdot)||_{\mathrm{TV}}$ equals 0? In light of the discussion below, one would expect that m_n would be on the order $\log n$. This has now been proven with a very clever argument in a recent preprint [5].

The original motivation for this paper comes from the results on mixing times for a number of classical shuffles; in particular, the *random to random insertion* shuffle, a random walk on S_n whose transition is implemented by choosing a card at random, removing it from the row, and then reinserting it in a random position in the row. Denote this random walk by $\{X_m\}_{m=0}^\infty$ and let $P_\sigma^{(n)}$ denote probabilities for the random walk starting from σ. The random walk is irreducible and the uniform distribution U_n is its invariant measure. It's aperiodic since $P_\sigma^{(n)}(X_1 = \sigma) = \frac{1}{n}$. Thus $P_{\mathrm{id}}^{(n)}(X_m \in \cdot)$ converges to U_n as $m \to \infty$. One is interested in the rate of convergence in the total variation norm as the parameter n grows. It is known that the mixing time is on the order $n \log n$. A long-standing open problem is to establish the *cut-off phenomenon*; namely to establish the existence of a c^* such that if $m_n \geq cn \log n$ with $c > c^*$, then $\lim_{n\to\infty} ||P^{(n)}_{\mathrm{id}}(X_{m_n} \in \cdot) - U_n||_{\mathrm{TV}} = 0$, and if $m_n \leq cn \log n$ with $c < c^*$, then $\lim_{n\to\infty} ||P^{(n)}_{\mathrm{id}}(X_{m_n} \in \cdot) - U_n||_{\mathrm{TV}} = 1$. It has been conjectured that $c^* = \frac{3}{4}$. Very recently, using very delicate probabilistic estimates [11], it has been proven that for any $\epsilon > 0$, $(\frac{3}{4} - \epsilon)n \log n$ shuffles is not enough to mix the deck. Using analytic methods, it was shown that for any $\epsilon > 0$, $(2 + \epsilon)n \log n$ shuffles does mix the deck [9]. Thus, if the cutoff phenomenon occurs, then c^* must satisfy $\frac{3}{4} \leq c^* \leq 2$. For other similar looking shuffles, such as the *random transposition shuffle* (where at each stage, two cards are selected independently—so the same card might be selected twice—and then their positions are swapped) and the *top to random insertion shuffle* (where at each stage, the current top card (left-most card in our setup) is removed and randomly reinserted), the cut-off phenomenon has been proven with m_n in the same form as above, with $c^* = \frac{1}{2}$ and $c^* = 1$ respectively [1].

Note that the mixing times of all the shuffles above are on the order $n \log n$. Now recall that the coupon collector's problem is the problem of determining how many samples of an IID random variable, distributed uniformly on $[n]$, are required until every number has been selected at least once. Denoting the required number of samples by T_n, it is well known that $\lim_{n\to\infty} P(T_n \geq n \log n + c_n n)$ equals 0 if $\lim_{n\to\infty} c_n = \infty$ and equals 1 if $\lim_{n\to\infty} c_n = -\infty$. More delicate estimates show that if $T_{n;k}$ denotes the number of samples required until all but k cards are selected once, then $\lim_{n\to\infty} P(T_{n,n^l} \geq (1-l)n \log n + c_n n)$ equals 0 or 1 with c_n as above. The coupon collector phenomenology is an integral part of the proofs of some of the results noted above. This leads one to wonder whether the order $n \log n$ for mixing in the above shuffles is caused exclusively by the coupon collector's phenomenology, that is exclusively by the fact that one needs order $n \log n$ shuffles to move most of the cards at least once, or whether this order is inherent in these shuffles for additional reasons. (Indeed, after order $n \log n$ shuffles, most of the cards have been removed and reinserted many times.) It was natural then to consider a shuffle that moved every card exactly once. To make such a model as close as possible in spirit to the random to random insertion shuffle, one should randomize the order in which the n cards are removed and reinserted exactly once. However, this seemed intractable, so we were led to study the problem presented in this paper, where the order in which the cards are removed and reinserted is not random, but rather is the original left to right order of the cards. As was noted, the fact that $n! \nmid n^n$ when $n \geq 3$ shows immediately that the distribution of our shuffle cannot be uniform after one shuffle. If one randomizes the order in which the n cards are removed and reinserted, then this argument breaks down. However, even this shuffle does not give the uniform distribution; indeed, one can check by hand that for $n = 3$, the resulting probabilities can take on the values $\frac{26}{162}$ and $\frac{28}{162}$.

The reason we use the terminology *card-cyclic* is that in the card-shuffling literature the term *cyclic to random shuffle* (by which one means cyclic to random transposition shuffle) is used for the shuffle where at step k one takes the card *currently in position* k mod n and transposes it with a random card. This kind of shuffle is *position-cyclic,* whereas ours is *card-cyclic.* In position cyclic shuffles, after one cycle, there are usually many cards that have not been moved at all. For results on position-cyclic to random transposition shuffles in the spirit of some of the results in this paper, see [8], [10], [3]. For results on position-cyclic to random transposition shuffles in the spirit of the question noted above from a prior preprint version of this paper, see [4] and [6].

We prove Theorems 1-6 in sections 2-7 respectively. The proofs of Corollaries 3, 4 and 5 are given immediately after the proof of Theorem 4.

2. Proof of Theorem 1

We will prove (1.1). With the exception of the final claim in the theorem that the total mass of a certain measure is equal to e^{-1}, the other claims in the statement of the theorem follow directly from (1.1).

To prove the above-mentioned final claim, we need to show that

$$\int_0^\infty \Big(\int_x^\infty e^{-\frac{1}{2}y^2}dy\Big)dx = 1. \tag{2.1}$$

Note that $F(x) \equiv \sqrt{\frac{2}{\pi}}\int_0^x e^{-\frac{1}{2}y^2}dy$ is the distribution function of $|Z|$, where $Z \sim \mathrm{N}(0,1)$. Thus

$$\int_0^\infty (1-F(x))dx = E|Z| = \sqrt{\frac{2}{\pi}}\int_0^\infty xe^{-\frac{1}{2}x^2}dx = \sqrt{\frac{2}{\pi}}. \tag{2.2}$$

But $1-F(x) = \sqrt{\frac{2}{\pi}}\int_x^\infty e^{-\frac{1}{2}y^2}dy$. Substituting this in (2.2) gives (2.1).

We now prove (1.1). We first derive the exact combinatorial formula for $p_n(\mathrm{id},\{\sigma_1 = j\})$. Of course we have $p_n(\mathrm{id},\{\sigma_1 = n\}) = \frac{1}{n}$. Now consider $1 \le j \le n-1$. If card number j is moved to the k-th position, with $2 \le k \le n-j+1$, then at the end of the shuffle it will be in the first position if and only if the following occur. Cards numbered 1 up to $j-1$, which were moved before card number j was moved, must move successively to the right of card number $j+k-1$. If this occurs, then after card number j is moved to position k, the cards numbered $j+1$ up to $j+k-1$ will be to the left of card number j. These cards numbered $j+1$ to $j+k-1$ now must move successively to the right of card number j. If this occurs, then card number j will be in the first position. Now cards numbered $j+k$ up to n must all move to positions greater or equal to two, so that card number j remains in the first position. We now calculate the probability of this occurring. The probability that cards numbered 1 up to $j-1$ move successively to the right of card number $j+k-1$ is $\prod_{l=2}^{j}\frac{n-j-k+l}{n}$. The probability that cards numbered $j+1$ to $j+k-1$, which occupy the first $k-1$ positions, move successively to the right of card number j, which occupies the k-th position, is $\prod_{l=1}^{k-1}\frac{n-k+l}{n}$. The probability that cards numbered $j+k$ up to n all move to positions greater or equal to two is $(\frac{n-1}{n})^{n-j-k+1}$. Thus, conditioned on card number j moving to position k, with $2 \le k \le n-j+1$, the probability that card number j will end up in the first position is $\frac{(n-1)!}{(n-j-k+1)!}\frac{(n-1)^{n-j-k+1}}{n^{n-1}}$. Conditioned on card number j moving to position k with $k > n-j+1$, the above considerations show that the probability of it ending up in the first position is zero.

Now consider the case that $k=1$; that is, j is moved to the first position. At the end of the shuffle, card number j will be in the first position if and only if the following occur. Cards numbered 1 up to $j-1$ may move unrestrictedly. Then after card number j is moved to the first position, cards numbered $j+1$ to n must move to positions greater or equal to two, so that card number j remains in the first position. Thus, conditioned on card j moving to the first position, the probability that it will end up in the first position is $(\frac{n-1}{n})^{n-j}$.

From the above considerations and calculations, we conclude that

$$\begin{aligned}
&p_n(\mathrm{id},\{\sigma_1=j\})=\frac{1}{n}(\frac{n-1}{n})^{n-j}+\frac{(n-1)!}{n^n}\sum_{k=2}^{n-j+1}\frac{(n-1)^{n-j-k+1}}{(n-j-k+1)!}=\\
&\frac{1}{n}(\frac{n-1}{n})^{n-j}+\frac{(n-1)!}{n^n}\sum_{\theta=j+1}^{n}\frac{(n-1)^{n-\theta}}{(n-\theta)!}.
\end{aligned} \tag{2.3}$$

Note that the above formula also holds for $j=n$, the resulting summation expression interpreted to be 0.

Let

$$S_{j,n}\equiv\frac{(n-1)!}{n^n}\sum_{\theta=j+1}^{n}\frac{(n-1)^{n-\theta}}{(n-\theta)!}. \tag{2.4}$$

We have

$$\begin{aligned}
&\frac{(n-1)!}{n^n}\frac{(n-1)^{n-\theta}}{(n-\theta)!}\le n^{-\theta}(n-1)(n-2)\cdots(n-(\theta-1))=\\
&=\frac{1}{n}(1-\frac{0}{n})(1-\frac{1}{n})\cdots(1-\frac{\theta-1}{n})\le\frac{1}{n}e^{-\frac{\theta(\theta-1)}{2n}}.
\end{aligned}$$

Thus, if $\theta\ge[n^{0.6}]+1$, then

$$\frac{(n-1)!}{n^n}\frac{(n-1)^{n-\theta}}{(n-\theta)!}\le\frac{1}{n}e^{-\frac{[n^{0.6}]^2}{2n}}=O(e^{-n^{0.1}}),\ \text{uniformly in }\theta\text{ as }n\to\infty.$$

so

$$\frac{(n-1)!}{n^n}\sum_{\theta=\max(j+1,[n^{0.6}]+1)}^{n}\frac{(n-1)^{n-\theta}}{(n-\theta)!}=O(e^{-n^{0.1}}),\ \text{uniformly in } j \text{ as } n\to\infty. \tag{2.5}$$

For $\theta \le n^{[.06]}$, we have from Stirling's formula,

(2.6)

$$\frac{(n-1)!}{n^n}\frac{(n-1)^{n-\theta}}{(n-\theta)!} = \frac{1}{n}\sqrt{2\pi n}(\frac{n}{en})^n\frac{1}{\sqrt{2\pi(n-\theta)}}(\frac{e(n-1)}{n-\theta})^{n-\theta}(1+O(\frac{1}{n})) =$$

$$\frac{1}{n}\sqrt{\frac{n}{n-\theta}}(1+O(\frac{1}{n}))e^{-\theta+(n-\theta)\log(1+\frac{\theta-1}{n-\theta})} =$$

$$\frac{1}{n}(1+O(n^{-0.4}))e^{-\theta+(\theta-1-\frac{1}{2}\frac{(\theta-1)^2}{n-\theta}+O(n^{-0.2})} = \frac{1}{en}e^{-\frac{1}{2}\frac{\theta^2}{n}}(1+O(n^{-0.2})), \text{ uniformly in } \theta.$$

Let

$$T_{j,n} \equiv \sum_{\theta=j+1}^{[n^{0.6}]} e^{-\frac{1}{2}\frac{\theta^2}{n}}.$$

Then if follows from (2.6) that

$$S_{j,n} = \frac{1}{en}T_{j,n}(1+O(n^{-0.2})) + O(e^{-n^{0.1}}), \text{ uniformly in } j \text{ as } n \to \infty. \tag{2.7}$$

Let

$$U_{j,n} \equiv \sum_{\theta=j+1}^{\infty} e^{-\frac{1}{2}\frac{\theta^2}{n}}.$$

Then clearly,

$$|T_{j,n} - U_{j,n}| \le \sum_{\theta=[n^{0.6}]+1}^{\infty} e^{-\frac{1}{2}\frac{\theta^2}{n}} = U_{[n^{0.6}],n}. \tag{2.8}$$

We have

$$\sum_{\theta=j+1}^{\infty}\int_{\frac{\theta}{\sqrt{n}}}^{\frac{\theta+1}{\sqrt{n}}} e^{-\frac{1}{2}x^2}dx \le \frac{U_{j,n}}{\sqrt{n}} \le \sum_{\theta=j+1}^{\infty}\int_{\frac{\theta-1}{\sqrt{n}}}^{\frac{\theta}{\sqrt{n}}} e^{-\frac{1}{2}x^2}dx,$$

so

$$\int_{\frac{j+1}{\sqrt{n}}}^{\infty} e^{-\frac{1}{2}x^2}dx \le \frac{U_{j,n}}{\sqrt{n}} \le \int_{\frac{j}{\sqrt{n}}}^{\infty} e^{-\frac{1}{2}x^2}dx. \tag{2.9}$$

Let

$$\psi(t) \equiv \int_t^{\infty} e^{-\frac{1}{2}x^2}dx, \ t \ge 0.$$

We have the inequality

$$\frac{1}{t+\sqrt{\frac{2}{\pi}}}e^{-\frac{1}{2}t^2} \le \psi(t) \le \frac{1}{t}e^{-\frac{1}{2}t^2}, \ t \ge 0. \tag{2.10}$$

The upper bound is well-known and follows from $\psi(t) \le \frac{1}{t}\int_t^\infty xe^{-\frac{1}{2}x^2}dx$, while the lower bound can be found in [7]. From (2.9) and (2.10) we have

$$U_{[n^{0.6}],n} \le \sqrt{n}\psi(\frac{[n^{0.6}]}{\sqrt{n}}) = O(e^{-n^{0.1}}), \text{ as } n \to \infty.$$

Thus, from (2.8) we have

$$T_{j,n} = U_{j,n} + O(e^{-n^{0.1}}), \text{ uniformly in } j \text{ as } n \to \infty, \tag{2.11}$$

and consequently from (2.7) we conclude that

$$S_{j,n} = \frac{1}{en}U_{j,n}(1 + O(n^{-0.2})) + O(e^{-n^{0.1}}), \text{ uniformly in } j \text{ as } n \to \infty. \tag{2.12}$$

We now show that we can replace $U_{j,n}$ above with $\sqrt{n}\psi(\frac{j}{\sqrt{n}})$. We break the estimate up into three different ranges of j. From (2.9) it follows that for all j,

$$|\frac{U_{j,n}}{\sqrt{n}} - \psi(\frac{j}{\sqrt{n}})| \le \frac{1}{\sqrt{n}}e^{-\frac{1}{2}\frac{j^2}{n}}. \tag{2.13}$$

From (2.13), if follows that

$$\frac{U_{j,n}}{\sqrt{n}} = \psi(\frac{j}{\sqrt{n}}) + O(e^{-n^{0.1}}), \text{ uniformly in } j \ge [n^{0.6}], \text{ as } n \to \infty. \tag{2.14}$$

On the other hand, if $j \le \sqrt{n}$, then $\psi(\frac{j}{\sqrt{n}}) \ge \psi(1)$ and $e^{-\frac{1}{2}\frac{j^2}{n}} \le 1$, so from (2.13) we have

$$\frac{U_{j,n}}{\sqrt{n}} = \psi(\frac{j}{\sqrt{n}})(1 + O(\frac{1}{\sqrt{n}})), \text{ uniformly in } j \le \sqrt{n}, \text{ as } n \to \infty. \tag{2.15}$$

Finally, consider $\sqrt{n} < j < [n^{0.6}]$. Then from (2.10) we have

$$\frac{\frac{1}{\sqrt{n}}e^{-\frac{1}{2}\frac{j^2}{n}}}{\psi(\frac{j}{\sqrt{n}})} = O(\frac{j}{n}) = O(n^{-0.4}), \text{ uniformly in } j \text{ for } \sqrt{n} < j < [n^{0.6}] \text{ as } n \to \infty. \tag{2.16}$$

Now (2.13) and (2.16) give

$$\frac{U_{j,n}}{\sqrt{n}} = \psi(\frac{j}{\sqrt{n}})(1 + O(n^{-0.4})), \text{ uniformly in } j \text{ for } \sqrt{n} < j < [n^{0.6}] \text{ as } n \to \infty. \tag{2.17}$$

From (2.14), (2.15), and (2.17), it follows that we can replace $U_{j,n}$ in (2.12) with $\sqrt{n}\psi(\frac{j}{\sqrt{n}})$ to obtain

(2.18)

$$S_{j,n} = \frac{1}{e\sqrt{n}}\psi(\frac{j}{\sqrt{n}})(1+O(n^{-0.2})) + O(e^{-n^{0.1}}), \text{ uniformly in } j \text{ as } n \to \infty.$$

Since

$$\frac{1}{n}(\frac{n-1}{n})^{n-j} = \frac{1}{n}e^{(n-j)\log(1-\frac{1}{n})} = \frac{1}{n}e^{\frac{j}{n}-1}(1+O(\frac{1}{n})), \text{ uniformly in } j \text{ as } n \to \infty,$$

it follows from (2.18), (2.4) and (2.3) that

(2.19)

$$p_n(\mathrm{id}, \{\sigma_1 = j\}) = \frac{1}{n}e^{\frac{j}{n}-1}(1+O(\frac{1}{n})) + \frac{1}{e\sqrt{n}}\psi(\frac{j}{\sqrt{n}})(1+O(n^{-0.2})) + O(e^{-n^{0.1}}),$$

uniformly in j as $n \to \infty$.

□

3. Proof of Theorem 2

We first derive the exact combinatorial formula for $p_n(\mathrm{id}, \{\sigma_n = j\})$. Of course, $p_n(\mathrm{id}, \{\sigma_n = n\}) = \frac{1}{n}$. Now consider $1 \le j \le n-1$. If card number j is moved to the k-th position, with $j \le k \le n$, then at the end of the shuffle it will be in the last position if and only if the following occur. Cards numbered 1 to $j-1$, which were moved before card number j was moved, must all move to the left of card number $k+1$ (if $k = n$, these cards can move unrestrictedly). If this occurs, then after card number j is moved to position k, the cards numbered $1, \cdots, j-1$ and $j+1, \cdots, k$ will be to the left of card number j. Now cards numbered $j+1, \cdots, k$ must all move to positions smaller or equal to $k-1$ in order that they remain to the left of card number j. And then cards numbered $k+1, \cdots, n$ must successively move to the left of card number j (if $k = n$, this step is vacuous). We now calculate the probability of this occurring. The probability that cards numbered 1 up to $j-1$ move to left of card number $k+1$ is $(\frac{k}{n})^{j-1}$. The probability that cards numbered $j+1, \cdots, k$, which are all in positions smaller than or equal to $k-1$, will all move to positions smaller than or equal to $k-1$ is $(\frac{k-1}{n})^{k-j}$. The probability that cards numbered $k+1, \cdots, n$, which occupy the positions $k+1, \cdots, n$, move successively to the left of card number j

which occupies the k-th position, is $\prod_{l=k}^{n-1}\frac{l}{n}$. Thus, conditioned on card number j moving to position k, with $j\le k\le n$, the probability that card number j will end up in the last position is $\frac{k^{j-1}(k-1)^{k-j}}{(k-1)!}\frac{(n-1)!}{n^{n-1}}$. Conditioned on card number j moving to position k with $1\le k\le j-1$, the above considerations show that the probability of it ending up in the last position is zero.

From the above considerations and calculations, we conclude that

$$p_n(\mathrm{id},\{\sigma_n=j\})=\frac{(n-1)!}{n^n}\sum_{k=j}^n\frac{k^{j-1}(k-1)^{k-j}}{(k-1)!},\tag{3.1}$$

which we rewrite in the form

$$p_n(\mathrm{id},\{\sigma_n=j\})=\frac{(n-1)!}{n^n}\sum_{m=j-1}^{n-1}\big(1+\frac{1}{m}\big)^{j-1}\ \frac{m^m}{m!},\tag{3.2}$$

where 0^0 and $(1+\frac{1}{0})^0$ are understood to be 1. Note that the formula is also correct for $j=n$. Let

$$S_{j,n}\equiv\sum_{m=j-1}^{n-1}\big(1+\frac{1}{m}\big)^{j-1}\ \frac{m^m}{m!}.\tag{3.3}$$

We will now always assume that $n\ge 4$. For all $m\ge j-1$, we have

$$(1+\frac{1}{m})^{j-1}\le(1+\frac{1}{j-1})^{j-1}\le e,$$

and for all m we have $m!\ge(\frac{m}{e})^m$. Thus,

$$(1+\frac{1}{m})^{j-1}\frac{m^m}{m!}\le e\frac{m^m}{(\frac{m}{e})^m}=e^{m+1}.$$

From this it follows that

$$\sum_{m=j-1}^{n-[\sqrt{n}]}\big(1+\frac{1}{m}\big)^{j-1}\ \frac{m^m}{m!}=O(e^{n-\sqrt{n}}),\ \text{uniformly in } j \text{ as } n\to\infty.\tag{3.4}$$

However, by Stirling's formula, the last term in the sum $S_{j,n}$ is at least $\frac{(n-1)^{n-1}}{(n-1)!}=\frac{1}{\sqrt{2\pi(n-1)}}e^{n-1}(1+o(1))$ as $n\to\infty$. Thus, it follows from (3.4) that

$$S_{j,n}=\Big(\sum_{m=\max(j-1,n-[\sqrt{n}]+1)}^{n-1}\big(1+\frac{1}{m}\big)^{j-1}\ \frac{m^m}{m!}\Big)\big(1+o(1)\big),\ \text{as } n\to\infty.\tag{3.5}$$

For the range of m being considered in (3.5), Stirling's formula gives

$m! = \sqrt{2\pi m}(\frac{m}{e})^m(1+o(1))$, uniformly in m and uniformly over all j as $n \to \infty$.

Also, uniformly in m for the range considered in (3.5),

$$(1+\frac{1}{m})^{j-1} = e^{(j-1)\log(1+\frac{1}{m})} = e^{(j-1)(\frac{1}{n}+O(n^{-\frac{3}{2}}))} = e^{\frac{(j-1)}{n}}(1+o(1)),$$

uniformly in j as $n \to \infty$.

We conclude then that

(3.6)

$$S_{j,n} = e^{\frac{j-1}{n}}\frac{1}{\sqrt{2\pi n}}\Big(\sum_{m=\max(j-1,n-[\sqrt{n}]+1)}^{n-1} e^m\Big)\big(1+o(1)\big), \text{ uniformly in } j \text{ as } n \to \infty.$$

From (3.6), (3.3), (3.2) and Stirling's formula, we conclude that

$$p_n(\mathrm{id}, \{\sigma_n = j\}) = \frac{1}{n}e^{\frac{j}{n}}\frac{1-e^{\max(j-1,n-[\sqrt{n}]+1)-n}}{e-1}\big(1+o(1)\big), \tag{3.7}$$

uniformly in j as $n \to \infty$.

The three parts of the theorem follow immediately from (3.7).

□

4. Proof of Theorem 3

Let $L, M > 0$, with L being an integer. In the calculations that follow, we will use the generic P to denote probabilities of events concerning the shuffling mechanism. Let $B_M^{(n)}$ be the event that at least one out of the first $[Mn^{\frac{1}{2}}]$ cards (that is, the cards numbered from 1 to $[Mn^{\frac{1}{2}}]$) gets removed and reinserted in a position that is no greater than $[Mn^{\frac{1}{2}}]$. Note that $P(B_M^{(n)}) = 1-(1-\frac{[Mn^{\frac{1}{2}}]}{n})^{[Mn^{\frac{1}{2}}]}$; so

$$\lim_{n\to\infty} P(B_M^{(n)}) = 1-e^{-M^2}. \tag{4.1}$$

If the event $B_M^{(n)}$ occurs, let $j_M^{(n)} \le [Mn^{\frac{1}{2}}]$ denote the number of the card with the smallest number that gets removed and reinserted in a position no greater than $[Mn^{\frac{1}{2}}]$. For convenience, we define $j_M^{(n)} = \infty$ if the event $B_M^{(n)}$ does not occur; thus, $B_M^{(n)} = \{j_M^{(n)} \le [Mn^{\frac{1}{2}}]\}$.

For $L < [Mn^{\frac{1}{2}}]-1$, define $C_{M,L}^{(n)}$ to be the event that no more than L out of the first $[Mn^{\frac{1}{2}}]$ cards are removed and reinserted in a position to the left of card number $2[Mn^{\frac{1}{2}}]-L-1$ (by the restriction on L, card number $2[Mn^{\frac{1}{2}}]-L-1$ is guaranteed not to be among the first $[Mn^{\frac{1}{2}}]$ cards). From the definitions, it is easy to see that

$$P(C^{(n)}_{M,L})\ge P(X_{n,M,L}\le L),$$

where $X_{n,M,L}\sim \text{Bin}([Mn^{\frac{1}{2}}],\frac{2[Mn^{\frac{1}{2}}]-L-2}{n})$. Since $EX_{n,M,L},\text{Var}(X_{n,M,L})\sim 2M^2$ as $n\to\infty$, it follows that

$$\lim_{M\to\infty}\lim_{n\to\infty}P(C^{(n)}_{M,L(M)})=1,\ \text{if}\ L(M)\ge 3M^2. \tag{4.2}$$

We claim that if $C^{(n)}_{M,L}$ occurs and $j^{(n)}_M\le[Mn^{\frac{1}{2}}]$, then immediately after card number $j^{(n)}_M$ is removed and reinserted, there will be no more than L cards with numbers less than $j^{(n)}_M$ appearing to the left of card number $j^{(n)}_M$. Indeed, assume to the contrary that at least $L+1$ cards with numbers less than $j^{(n)}_M$ appear to the left of newly reinserted card number $j^{(n)}_M$. But then since $C^{(n)}_{M,L}$ has occurred, card number $2[Mn^{\frac{1}{2}}]-L-1$ is also necessarily to the left of newly reinserted card number $j^{(n)}_M$. Since every card with a number greater than $[Mn^{\frac{1}{2}}]$ has not yet been removed and reinserted, it follow that all these cards maintain their original relative order; thus in fact all the cards from $[Mn^{\frac{1}{2}}]+1$ up to $2[Mn^{\frac{1}{2}}]-L-1$ are to the left of newly reinserted card number $j^{(n)}_M$. We conclude that these $[Mn^{\frac{1}{2}}]-L-1$ cards as well as at least $L+1$ other cards are to the left of newly inserted card number $j^{(n)}_M$; but this contradicts the assumption that the position of card number $j^{(n)}_M$ is no greater than $[Mn^{\frac{1}{2}}]$.

If $j^{(n)}_M\le[Mn^{\frac{1}{2}}]$, let $\text{pos}(j^{(n)}_M)$ denote its position immediately after it is removed and reinserted. For the rest of this paragraph, when we use the word "now," we mean at the time immediately after card $j^{(n)}_M$ is removed and reinserted. If $j^{(n)}_M\le[Mn^{\frac{1}{2}}]$ and $C^{(n)}_{M,L}$ has occurred, then immediately after card number $j^{(n)}_M$ is removed and reinserted, it will find itself in position $\text{pos}(j^{(n)}_M)\le[Mn^{\frac{1}{2}}]$, and the number of cards with lower numbers than $j^{(n)}_M$ that will be occupying positions to the left of position $\text{pos}(j^{(n)}_M)$ will be between 0 and L; call this number L'. All the cards with numbers higher than $j^{(n)}_M$ will be in their original relative order; thus, $\text{pos}(j^{(n)}_M)-1-L'$ of them will be in positions to the left of $\text{pos}(j^{(n)}_M)$, and $n-j^{(n)}_M-\text{pos}(j^{(n)}_M)+1+L'$

of them will be in positions to the right of $\mathrm{pos}(j_M^{(n)})$. Let $D_{M,L}^{(n)}$ denote the event that no more than L out of these $\mathrm{pos}(j_M^{(n)})-1-L'$ cards that are now to the left of card $j_M^{(n)}$ in position $\mathrm{pos}(j_M^{(n)})$ end up to the left of card $j_M^{(n)}$ after being removed and reinserted, and let $E_{M,L,\rho}^{(n)}$ denote the event that no more than ρL out of these $n-j_M^{(n)}-\mathrm{pos}(j_M^{(n)})+1+L'$ cards that are now to the right of card $j_M^{(n)}$ in position $\mathrm{pos}(j_M^{(n)})$ end up to the left of card $j_M^{(n)}$ after they are finally removed and reinserted, thereby ending the shuffle. Here ρL is an integer.

By looking at the worst case scenario (by choosing $L'=0$ and $\mathrm{pos}(j_M^{(n)}) = [Mn^{\frac{1}{2}}]$), it follows easily that

$$P(D_{M,L}^{(n)}|C_{M,L}^{(n)}, B_M^{(n)}) \geq P(Y_{n,M,L} \leq L),$$

where $Y_{n,M,L} \sim \mathrm{Bin}([Mn^{\frac{1}{2}}]-1, \frac{[Mn^{\frac{1}{2}}]-1}{n})$. Since $EY_{n,M,L}, \mathrm{Var}(Y_{n,M,L}) \sim M^2$ as $n \to \infty$, it follows that

$$\lim_{M\to\infty}\lim_{n\to\infty} P(D_{M,L(M)}^{(n)}|C_{M,L(M)}^{(n)}, B_M^{(n)}) = 1, \text{ if } L(M) \geq 2M^2. \tag{4.3}$$

Now we consider $P(E_{M,L,\rho}^{(n)}|D_{M,L}^{(n)}, C_{M,L}^{(n)}, B_M^{(n)})$. Conditioned on $B_M^{(n)}, C_{M,L}^{(n)}$ and $D_{M,L}^{(n)}$, when event $D_{M,L}^{(n)}$ ends and event $E_{M,L,\rho}^{(n)}$ starts, the card $j_M^{(n)}$ will be in a position between 1 and $2L+1$; call the position k. Then the worst case scenario would be to set $n-j_M^{(n)}-\mathrm{pos}(j_M^{(n)})+1+L'$ equal to $n-k$; that is, equal to the total number of cards to the right of card $j_M^{(n)}$. Thus a lower bound for $P(E_{M,L,\rho}^{(n)}|D_{M,L}^{(n)}, C_{M,L}^{(n)}, B_M^{(n)})$ is the minimum over those k between 1 and $2L+1$ of the probability that in a deck of n cards ordered from 1 to n, if one removes and randomly reinserts the last $n-k$ cards, then no more than ρL of them get reinserted to the left of card k. We can write these probabilities in terms of certain probabilities for certain geometric random variables. For any $i \geq 1$, let $T_{q_i}^i$ denote a geometric random variable with parameter q_i and with values in $\{1, 2, \cdots\}$, and let $T_{q_i}^i$ and $T_{q_j}^j$ be independent for $j \neq i$. For a fixed k, the above probability is $P(\sum_{l=0}^{\rho L} T_{\frac{k+l}{n}} > n-k)$. To see this, think of the number of cards that are removed and randomly reinserted until the first time one of them gets placed to the left of card number k as a $T_{\frac{k}{n}}^1$ random variable, think of the number of cards after the first one gets placed to the left of card number j

until a second one gets placed to the left of card number j as a $T^2_{\frac{k+1}{n}}$ random variable, etc. (In fact, these numbers are not distributed according to these random variables, because there are only a finite number of cards. What is true precisely, for example, with regard to the first time a card gets placed to the left of card number k is that for $l \le n-k$, the probability of needing exactly l cards to be removed and reinserted until the first time one of them gets placed to the left of card number k is equal to the probability that $T^1_{\frac{k}{n}}$ is equal to l.)

So we have

$$P(E^{(n)}_{M,L,\rho}|D^{(n)}_{M,L},C^{(n)}_{M,L},B^{(n)}_M) \ge \min_{1\le k\le 2L+1} P(\sum_{l=0}^{\rho L} T_{\frac{k+l}{n}} > n-k). \tag{4.4}$$

Now for all $0 \le k \le 2L+1$,

$$E\sum_{l=0}^{\rho L} T_{\frac{k+l}{n}} = n\sum_{l=0}^{\rho L}\frac{1}{k+l} \ge n\log\frac{k+\rho L+1}{k} \ge n\log\frac{2L+2+\rho L}{2L+1},$$

and

$$\mathrm{Var}(\sum_{l=0}^{\rho L} T_{\frac{k+l}{n}}) \le Cn^2,$$

for a constant C_0 independent of k and L. Thus, by Chebyshev's inequality, for any $\lambda(L)$,

$$P(\sum_{l=0}^{\rho L} T_{\frac{k+l}{n}} \ge n\log\frac{2L+2+\rho L}{2L+1} - n\lambda(L)) \ge 1 - \frac{C_0}{(\lambda(L))^2}. \tag{4.5}$$

Let ρ be sufficiently large so that $\log\frac{2+\rho}{2} > 2$. Then $\log\frac{2L+2+\rho L}{2L+1} > 2$, for sufficiently large L. Thus, letting $\lambda(L) = \frac{1}{2}\log\frac{2L+2+\rho L}{2L+1}$, it follows from (4.4) and (4.5) that

$$\lim_{L\to\infty}\lim_{n\to\infty} P(E^{(n)}_{M,L,\rho}|D^{(n)}_{M,L},C^{(n)}_{M,L},B^{(n)}_M) \ge 1 - \frac{C_0}{(\frac{1}{2}\log\frac{2+\rho}{2})^2}. \tag{4.6}$$

If events $B^{(n)}_M, C^{(n)}_{M,L}$, $D^{(n)}_{M,L}$ and $E^{(n)}_{M,L,\rho}$ occur, then at the end of the shuffle, card number $j^{(n)}_M \le [Mn^{\frac{1}{2}}]$ will end up in a position between 1 and $2L+\rho L+1$. Thus, by (4.1)-(4.3) and (4.6), we conclude that (1.7) holds.

Finally, we have $U_n(A^{(n)}_{M,L}) = 1 - \frac{\binom{n-[Mn^{\frac{1}{2}}]}{L}}{\binom{n}{L}}$, from which it follows that $\lim_{n\to\infty} U_n(A^{(n)}_{M,L}) = 0$. This in conjunction with (1.7) proves (1.8). $\square$

5. Proofs of Theorem 4 and Corollaries 3, 4 and 5

Proof of Theorem 4. Let b_n satisfy $\lim_{n\to\infty} b_n = b \in (0,1)$ with $b_n n$ an integer, and let d_n satisfy $\lim_{n\to\infty} d_n = d \in (0,1)$, w ith $d_n n$ an integer. Let $Q^{(n)}_{b_n,d_n}(x)$, $0 \le x \le 1$, denote the rescaled distribution function of $\sigma^{-1}_{b_n n}$ under $p_n(\mathrm{id},\cdot)$, when conditioned on card $b_n n$ having been removed and reinserted in position $d_n n$; that is

$$Q^{(n)}_{b_n,d_n}(x) = p_n(\mathrm{id}, \sigma^{-1}_{b_n n} \le nx|\text{card } b_n n \text{ was reinserted in position } d_n n).$$

Let $G_b(y)$ be as in the statement of the theorem. We will show that if $d \neq 1-(1-b)e^b$, then the distribution $Q^{(n)}_{b_n,d_n}(dx)$ corresponding to the distribution function $Q^{(n)}_{b_n,d_n}(x)$ converges weakly to the δ-distribution at $G_b(d)$:

$$w - \lim_{n\to\infty} Q^{(n)}_{b_n,d_n}(dx) = \delta_{G_b(d)}, \quad d \neq 1-(1-b)e^b. \tag{5.1}$$

It is easy to check that the function $G_b(y)$ is increasing in $y \in [0,1]$. Thus, since the probability that card $b_n n$ is inserted in a position no larger than $d_n n$ is d_n, it follows that $F_b(G_b(d)) = d$; that is, $G_b = F_b^{-1}$. Thus, to complete the proof of the theorem, we need to prove (5.1).

We use the generic P to denote probabilities of events concerning the shuffling mechanism, conditioned on card $b_n n$ having been removed and reinserted in position $d_n n$. For notational convenience, we will sometimes write $j = b_n n$ and $k = d_n n$. After card number j is removed and reinserted in position k, a certain number of cards from among those with numbers less than j (which were removed and reinserted before j was) will be to the left of newly reinserted card number j. Denote this random number of cards by M. Of course then, the other cards to the left of newly reinserted card number j are the cards $j+1, \cdots, j+k-1-M$. These cards are the next to be removed and reinserted. Let R denote the random number of cards out of these $k-1-M$ cards that end up to the left of card number j. So now card j is in position $M+R+1$. Now it is the turn of the remaining $n-j-k+M+1$ cards, with numbers from $j+k-M$ up to n, all of which are to the right of card number j, to be removed and reinserted. Let S denote the random number of cards out of these cards that end up to the left of card number j. Then at the end of the shuffle, card number j will be in position $M+R+S+1$.

We will show that if $d\neq 1-(1-b)e^b$, then as $n\to\infty$, the distribution of $\frac{M}{n}$ converges weakly to $\delta_{\gamma(b,d)}$, where

$$\gamma=\gamma(b,d)=\begin{cases} b-(1-d)(1-e^{-b}), & \text{if } d>1-(1-b)e^b;\\ d, & \text{if } d<1-(1-b)e^b.\end{cases} \tag{5.2}$$

Note that $\gamma(b,d)>0$ for all $0<b,d<1$. Assume now that $d\neq 1-(1-b)e^b$. We will show that as $n\to\infty$, the distribution of $\frac{R}{n}$ converges weakly to $\delta_{1-\gamma-(1-d)e^{d-\gamma}}$. Let $t=t(\gamma,d)=1-\gamma-(1-d)e^{d-\gamma}$. We will show that as $n\to\infty$, the distribution of $\frac{S}{n}$ converges weakly to $\delta_{(\gamma+t)(e^{1-b-d+\gamma}-1)}$. Thus $Q^{(n)}_{b_n,d_n}$, the rescaled distribution of the final position of card j, namely, the distribution of $\frac{M+R+S+1}{n}$, will converge to $\delta_{\gamma+t+(\gamma+t)(e^{1-b-d+\gamma}-1)}$. Using the equations above to write everything only in terms of b and d, we obtain

$$\gamma+t+(\gamma+t)(e^{1-b-d+\gamma}-1)=\begin{cases} de^{1-b}, & \text{if } d<1-(1-b)e^b;\\ e^{(1-d)e^{-b}}-(1-d)e^{1-b}, & \text{if } d>1-(1-b)e^b,\end{cases}$$

thus giving (5.1).

We now prove the claims in the above paragraph regarding the distributions of $\frac{M}{n}$, $\frac{R}{n}$ and $\frac{S}{n}$. We start with $\frac{M}{n}$. We consider the probability that $M=m$. From the definitions, it follows that in order for this probability to be nonzero, we need $0\le m\le \min(j-1,k-1)$ and $j-1-m\le n-k$. In the sequel, these restrictions will be assumed. A careful analysis of the shuffle up until the time that card number j is removed and reinserted in position k will reveal that if $j\le k$ and $0\le m\le j-1$, or if $k<j$ and $0\le m\le k-2$, then the random variable M will be equal to m if and only if at least m cards from among the first $j-1$ cards were inserted to the left of card number $j+k-m$, and at most m cards from among the first $j-1$ cards were inserted to the left of card number $j+k-m-1$. However if $k<j$ and $m=k-1$, then the random variable M will be equal to $m=k-1$ if and only if at least $m=k-1$ out of the first $j-1$ cards were inserted to the left of card number $j+1$.

Let $B_{n,j,k;m}$ denote the event that at most m cards from among the first $j-1$ cards were inserted to the left of card number $j+k-m-1$. From the previous paragraph, it follows that except for the boundary case $m=k-1$, one has $B_{n,j,k;m}=\{M\le m\}$.

We can express the probability $P(B_{n,j,k;m})$ in terms of certain probabilities for certain geometric random variables. For any $i\ge 0$, let $T^i_{q_i}$ denote a geometric random variable with parameter q_i and with values in $\{1,2,\cdots\}$, and let $T^i_{q_i}$ and $T^j_{q_j}$ be independent for $j\ne i$. we have

$$P(B_{n,j,k;m})=P(\sum_{l=1}^{j-m-1}T^l_{1-\frac{j+k-m-l-1}{n}}\le j-1),\ \text{as } n\to\infty. \tag{5.3}$$

The explanation for this is similar to that given at the point in the proof of Theorem 3 where geometric random variables were introduced. (Think of the number of cards that are removed and reinserted until the first time one of them gets placed to the *right* of card number $j+k-m-1$ as a $T^1_{1-\frac{j+k-m-2}{n}}$ random variable, think of the number of cards that are removed and reinserted after the first one gets placed to the right of card number $j+k-m-1$ until a second one gets placed to the right of card number $j+k-m-1$ as a $T^2_{1-\frac{j+k-m-3}{n}}$, etc., with the same caveat as noted in the proof of Theorem 3.)

We now note a fact that will be used several times below. If for each positive integer n, $\{T^l_{p_{n,l}}\}_{l=1}^{m_n}$ are independent geometric random variables, where m_n is a positive integer, and if

$$\liminf_{n\to\infty}\min_{1\le l\le m_n}p_{n,l}>0\ \text{ and }\ \mu\equiv\lim_{n\to\infty}\frac{1}{n}\sum_{l=1}^{m_n}ET^l_{p_{n,l}}\ \text{ exists,} \tag{5.4}$$

then a direct application of Chebyshev's inequality shows that $\frac{1}{n}\sum_{l=1}^{m_n}T^l_{p_{n,l}}$ converges weakly to μ.

Recall that $j=b_nn$ and $k=d_nn$. Write m in the form $m=\gamma_nn$ and assume that $\gamma=\lim_{n\to\infty}\gamma_n$ exists. By the restrictions on m noted earlier, we may assume that $\gamma\le\min(b,d)$. Note that (5.4) holds for $\{T^l_{1-\frac{j+k-m-l-1}{n}}\}_{l=1}^{j-m-1}$, if $b+d-\gamma<1$. Assume that this condition holds now. Then by the weak law of large numbers, it follows that $\frac{1}{n}\sum_{l=1}^{j-m-1}T^l_{1-\frac{j+k-m-l-1}{n}}$ converges weakly to its limiting expected value. The expected value of the above sum is $\frac{1}{n}\sum_{l=1}^{(b_n-\gamma_n)n}\frac{1}{1-b_n-d_n+\gamma_n+\frac{l+1}{n}}$; thus the limiting expected value is $\int_0^{b-\gamma}\frac{1}{1-b-d+\gamma+x}dx=\log\frac{1-d}{1-d-b+\gamma}$. On the other hand, $\lim_{n\to\infty}\frac{j-1}{n}=b$. Thus, from (5.3) we obtain

$$\lim_{n\to\infty}P(B_{n,j,k;m})=\begin{cases}1, \text{ if } \log\frac{1-d}{1-d-b+\gamma}<b;\\ 0, \text{ if } \log\frac{1-d}{1-d-b+\gamma}>b.\end{cases} \tag{5.5}$$

Recall that $B_{n,j,k;m}=\{M\le m\}$ except for the boundary case $m=k-1$. In this boundary case, we have $d=\gamma$. So we conclude from (5.5) that if $\gamma<d$ and $b+d-\gamma<1$, then $\frac{M}{n}$ converges weakly to the γ satisfying $\log\frac{1-d}{1-d-b+\gamma}=b$; that is, to $\gamma=b-(1-d)(1-e^{-b})$. This value of γ indeed satisfies $b+d-\gamma<1$. It will satisfy $\gamma<d$ if and only if $b-(1-d)(1-e^{-b})<d$; that is, if and only if $d>1-(1-b)e^b$. This gives the first possibility in (5.2).

If on the other hand, $d<1-(1-b)e^b$, then one can check that necessarily $d<b$, and thus we may assume that $k<j$. As noted above, if $k<j$ and $m=k-1$, then the random variable M will equal m if and only if at least $m=k-1$ out of the first $j-1$ cards were inserted to the left of card number $j+1$. Let $A_{n,j,k;k-1}$ denote the event that at least $k-1$ cards from among the first $j-1$ cards were inserted to the left of card number $j+1$; so $\{M=k-1\}=A_{n,j,k;k-1}$. Using the same kind of reasoning as in (5.3), we have

$$P(A_{n,j,k;k-1})=P(\sum_{l=1}^{j-k+1}T^l_{1-\frac{j+1-l}{n}}>j-1). \tag{5.6}$$

Since $m=k-1$, $m=\gamma_n n$ and $k=d_n n$, it follows that $\gamma=d$. Note that (5.4) holds for $\{T^l_{1-\frac{j+1-l}{n}}\}_{l=1}^{j-k+1}$. Thus, by the weak law of large numbers it follows that $\frac{1}{n}\sum_{l=1}^{j-k+1}T^l_{1-\frac{j+1-l}{n}}$ converges weakly to its limiting expected value. The expected value of the sum is $\frac{1}{n}\sum_{l=1}^{(b_n-d_n)n+1}\frac{1}{1-b_n+\frac{l-1}{n}}$; thus the limiting expected value is $\int_0^{b-d}\frac{1}{1-b+x}dx=\log\frac{1-d}{1-b}$. On the other hand, $\lim_{n\to\infty}\frac{j-1}{n}=b$. Thus, we conclude from (5.6) that

$$\lim_{n\to\infty}P(A_{n,j,k;k-1})=\begin{cases}1, \text{ if } \log\frac{1-d}{1-b}>b;\\ 0, \text{ if } \log\frac{1-d}{1-b}<b.\end{cases} \tag{5.7}$$

The inequality $\log \frac{1-d}{1-b} > b$ is equivalent to $d < 1-(1-b)e^b$, which is exactly the assumption we have made in this paragraph. Since $\{M = k-1\} = A_{n,j,k;k-1}$, we conclude that if $d < 1-(1-b)e^b$, then $\frac{M}{n}$ converges weakly to d. This gives the second possibility in (5.2). This completes the proof that if $d \neq 1-(1-b)e^b$, then the distribution of $\frac{M}{n}$ converges weakly to $\delta_{\gamma(b,d)}$, where $\gamma(b,d)$ is given by (5.2).

Now we turn to the distribution of $\frac{R}{n}$. Recall that as we begin to implement the random variable R, card number j is in position k, to the left of card number j are M cards that have already been removed and reinserted, as well as $k-M-1$ cards that are now to be removed and reinserted. The random variable R is the number of these $k-M-1$ cards that end up to the left of card number j. For the calculation below, let $\lambda_n n$ denote a possible value for M, and assume that $\lambda \equiv \lim_{n\to\infty} \lambda_n$ exists. Using geometric random variables, similar to the case for the random variable M, we have

$$P(\frac{R}{n} \leq t | M = \lambda_n n) = P(\sum_{l=1}^{k-\lambda_n n-1-tn} T^l_{1-\frac{k-l}{n}} \leq k - \lambda_n n - 1).$$

Note that (5.4) holds for $\{T^l_{1-\frac{k-l}{m}}\}_{l=1}^{k-\lambda_n n-1-tn}$ Thus, by the weak law of large numbers, it follows that $\frac{1}{n}\sum_{l=1}^{k-\lambda_n n-1-tn} T^l_{1-\frac{k-l}{n}}$ converges weakly to its limiting expected value, which is $\int_0^{d-\lambda-t} \frac{1}{1-d+x} dx = \log \frac{1-\lambda-t}{1-d}$. On the other hand $\lim_{n\to\infty} \frac{k-\lambda_n n-1}{n} = d - \lambda$. Thus, we conclude that

$$\lim_{n\to\infty} P(\frac{R}{n} \leq t | M = \lambda_n n) = \begin{cases} 1, \text{ if } \log \frac{1-\lambda-t}{1-d} < d - \lambda; \\ 0, \text{ if } \log \frac{1-\lambda-t}{1-d} > d - \lambda. \end{cases}$$

This proves that the distribution of $\frac{R}{n}$, conditioned on $M = \lambda_n n$, converges weakly to the δ-distribution at the $t = t(\lambda, d)$ which solves the equation $\log \frac{1-\lambda-t}{1-d} = d - \lambda$. The solution is $t(\lambda, d) = 1 - \lambda - (1-d)e^{d-\lambda}$. Since in fact, if $d \neq 1-(1-b)e^b$, the distribution of $\frac{M}{n}$ converges weakly to the δ-distribution at $\gamma = \gamma(b,d)$ given in (5.2), we conclude that if $d \neq 1-(1-b)e^b$, the distribution of $\frac{R}{n}$ converges weakly to the δ-distribution at $t = t(\gamma, d) = 1 - \gamma - (1-d)e^{d-\gamma}$, with $\gamma = \gamma(b,d)$.

We now turn to the distribution of $\frac{S}{n}$. Recall that as we begin to implement the random variable S, card number j is in position $M + R + 1$, and there are $n-j-k+M+1$ cards, all to the right of card number j, which need to be removed and reinserted. The random variable S is the number of these $n-j-k+M+1$ cards that end up to the left of card j. For the calculation below, let $\lambda_n n$ denote a possible value for M, let $\mu_n n$ denote a possible value for R, and assume that $\lambda\equiv\lim_{n\to\infty}\lambda_n>0$ exists and that $\mu\equiv\lim_{n\to\infty}\mu_n$ exists. Using geometric random variables again, we have

$$P(\frac{S}{n}\le v|M=\lambda_n n,R=\mu_n n)=P(\sum_{l=1}^{vn+1}T^l_{\lambda_n+\mu_n+\frac{l}{n}}>n-j-k+\lambda_n n+1).$$

Since we are assuming that $\lambda>0$, it follows that (5.4) holds for $\{T^l_{\lambda_n+\mu_n+\frac{l}{n}}\}_{l=1}^{vn+1}$. Thus, by the weak law of large numbers, it follows that $\frac{1}{n}\sum_{l=1}^{vn+1}T^l_{\lambda_n+\mu_n+\frac{l}{n}}$ converges weakly to its limiting expected value, which is $\int_0^v\frac{1}{\lambda+\mu+x}dx=\log\frac{\lambda+\mu+v}{\lambda+\mu}$. On the other hand, $\lim_{n\to\infty}\frac{n-j-k+\lambda_n n+1}{n}=1-b-d+\lambda$. Thus, we conclude that

$$\lim_{n\to\infty}P(\frac{S}{n}\le v|M=\lambda_n n,R=\mu_n n)=\begin{cases}1, \text{ if } \log\frac{\lambda+\mu+v}{\lambda+\mu}>1-b-d+\lambda;\\ 0, \text{ if } \log\frac{\lambda+\mu+v}{\lambda+\mu}<1-b-d+\lambda.\end{cases}$$

This proves that the distribution of $\frac{S}{n}$, conditioned on $M=\lambda_n n$ and $R=\mu_n n$, converges weakly to the δ-distribution at the $v=v(\lambda,\mu)$ which solves the equation $\log\frac{\lambda+\mu+v}{\lambda+\mu}=1-b-d+\lambda$. The solution is $v=v(\lambda,\mu,b,d)=(\lambda+\mu)(e^{1-b-d+\lambda}-1)$. Since the distribution of $\frac{M}{n}$ converges weakly to the δ-distribution at $\gamma=\gamma(b,d)>0$, and since the distribution of $\frac{R}{n}$ converges weakly to the δ-distribution at $t=t(\gamma,d)$, it follows that the distribution of $\frac{S}{n}$ converges weakly to the δ-distribution at $v(\gamma,t,b,d)=(\gamma+t)(e^{1-b-d+\gamma}-1)$, with $\gamma=\gamma(b,d)$ and $t=t(\gamma,d)$. □

Proof of Corollary 3. The proof of Theorem 4 shows that with regard to the position of a particular card at the end of the shuffle, the only randomness that remains when $n\to\infty$ is the randomness incurred by removing and reinserting that particular card, and not the randomness incurred by removing and reinserting other cards. Furthermore, as is clear intuitively and also from the above proof, a finite number of changes with regard to the positions of other cards does not change the limiting distribution of the card in question. The corollary follows from these facts. □

Proof of Corollary 4. First we prove part (i). Since $P(\Sigma_{1,b_1}^{-1} \leq \Sigma_{2,b_1}^{-1}) = \frac{1}{2}$, to prove part (i) it suffices to show that $\frac{dP(\Sigma_{1,b_1}^{-1} \leq \Sigma_{2,b_2}^{-1})}{db_2} |_{b_2=b_1} = (1-b_1)e^{b_1} - \frac{1}{2}$. We have

(5.8)
$$P(\Sigma_{1,b_1}^{-1} \leq \Sigma_{2,b_2}^{-1}) = \int_{0\leq x\leq y\leq 1} f_{b_1}(x) f_{b_2}(y) dy dx = \int_0^1 f_{b_1}(x)(1 - F_{b_2}(x))dx.$$

From the equation $G_b(F_b(x)) = x$, we obtain

$$\frac{dF_b}{db}(x) = -\frac{\frac{dG_b}{db}(F_b(x))}{G_b'(F_b(x))}.$$

Differentiating (5.8) with respect to b_2 and using the above equation along with the fact that $f_b(x) = \frac{1}{G_b'(F_b(x))}$, we have

$$\frac{dP(\Sigma_{1,b_1}^{-1} \leq \Sigma_{2,b_2}^{-1})}{db_2} |_{b_2=b_1} = \int_0^1 \frac{\frac{dG_b}{db} |_{b=b_1} (F_{b_1}(x))}{\left(G_{b_1}'(F_{b_1}(x))\right)^2} dx.$$

Making the substitution $x = G_{b_1}(y)$ in the above equation, we obtain

$$\frac{dP(\Sigma_{1,b_1}^{-1} \leq \Sigma_{2,b_2}^{-1})}{db_2} |_{b_2=b_1} = \int_0^1 \frac{\frac{dG_b}{db} |_{b=b_1} (y)}{G_{b_1}'(y)} dy. \tag{5.9}$$

Recalling the definition of G_b from Theorem 4, we have

$$\frac{dG_b}{db} = \begin{cases} -ye^{1-b}, & 0 \leq y \leq 1-(1-b)e^b; \\ (1-y)\left(e^{1-b} - e^{-b}e^{(1-y)e^{-b}}\right), & 1-(1-b)e^b \leq y \leq 1, \end{cases}$$

and

$$G_b'(y) = \begin{cases} e^{1-b}, & 0 \leq y \leq 1-(1-b)e^b; \\ e^{1-b} - e^{-b}e^{(1-y)e^{-b}}, & 1-(1-b)e^b \leq y \leq 1. \end{cases}$$

Note then that the quotient $\frac{\frac{dG_b}{db}|_{b=b_1}(y)}{G_{b_1}'(y)}$ reduces to $-y$ on $0 \leq y \leq 1-(1-b_1)e^{b_1}$, and reduces to $1-y$ on $1-(1-b_1)e^{b_1} \leq y \leq 0$. Thus, from (5.9), we obtain

$$\frac{dP(\Sigma_{1,b_1}^{-1} \leq \Sigma_{2,b_2}^{-1})}{db_2} |_{b_2=b_1} = -\int_0^{1-(1-b_1)e^{b_1}} y dy + \int_{1-(1-b_1)e^{b_1}}^1 (1-y) dy =$$
$$(1-b_1)e^{b_1} - \frac{1}{2}.$$

Now we prove part (ii). Recall that $f_1(x) \equiv 1$. Thus,

$$P(\Sigma_{1,b}^{-1} \leq \Sigma_{2,1}^{-1}) = \int_{0 \leq x \leq y \leq 1} f_b(x) dy dx = \int_0^1 (1-x) f_b(x) dx = 1 - E(b),$$

where $E(b)$ is as in Corollary 2. Furthermore, from that corollary, it follows that $E(b) > \frac{1}{2}$ for $b \in (\tilde{b}, 1)$ and $E(b) < \frac{1}{2}$, for $b \in [0, \tilde{b})$, where $\tilde{b}$ is the unique $b \in [0,1)$ for which $E(b) = \frac{1}{2}$. □

Proof of Corollary 5. Since $h_x(b) = f_b(x)$, the statements regarding $h_0(b)$ and $h_1(b)$ as well as statement (ii) follow from Corollary 1 and the definition of b_x.

For the proof of statement (i), write $x = G_b(y), y = F_b(x)$. In the range $0 < b < b_x$, we have $x > x_b = e^{1-b} - (1-b)e$, so $y > F_b(x_b) = 1 - (1-b)e^b$, and

$$x = G_b(y) = e^{\phi} - e\phi, \text{ where } \phi \equiv (1-y)e^{-b}. \tag{5.10}$$

Therefore,

$$h_x(b) = f_b(x) = \frac{\partial F_b}{\partial x} = \frac{1}{\frac{\partial G_b}{\partial y}} = \frac{1}{\frac{\partial G_b}{\partial \phi} \frac{\partial \phi}{\partial y}} = \frac{e^b}{e - e^{\phi}}. \tag{5.11}$$

However, from (5.10), ϕ depends only on x, and not on b, so if $0 < b < b_x$, then

$$\frac{\partial h_x(b)}{\partial b} = h_x(b). \tag{5.12}$$

Thus

$$h_x(b) = c_x e^b, \ 0 < b < b_x,$$

for some c_x. We now evaluate c_x. We have $f_0(x) = \frac{1}{G_0'(G_0^{-1}(x))}$, and $G_0'(y) = e - e^{1-y}$. Note that $G_0(y)$ and x_b are the same function (one of y and one of b). Thus, $h_x(0^+) = h_x(0) = f_0(x) = \frac{1}{e - e^{1-b_x}} = \frac{e^{b_x - 1}}{e^{b_x} - 1}$. Consequently, $c_x = \frac{e^{b_x - 1}}{e^{b_x} - 1}$. □

6. Proof of Theorem 5

To prove the theorem, we will need to consider a related shuffle. Fix two (not necessarily distinct) permutations $\sigma, \tau \in S_n$. Start the deck from σ and then use τ in the following manner to remove and randomly reinsert each card exactly once: for each $j = 1, \cdots, n$, the j-th card to be removed and randomly reinserted is the card with the number τ_j on it. Let $p_n^\tau(\sigma,\cdot)$ denote the resulting distribution. (Note that in terms of these shuffles, we have $p_n(\sigma,\cdot) = p^\sigma(\sigma,\cdot)$; in particular, $p_n(\mathrm{id},\cdot) = p^{\mathrm{id}}(\mathrm{id},\cdot)$.) Let $\mathrm{id}^{\mathrm{opp}}$ denote the permutation in S_n satisfying $\mathrm{id}_j^{\mathrm{opp}} = n-j+1$, $j = 1,\cdots,n$. Note then that $p_n^{\mathrm{id}^{\mathrm{opp}}}(\sigma,\mathrm{id})$ is the probability of ending up with the identity permutation, if one starts from σ and removes and reinserts the cards one by one, in the order $n, n-1,\cdots,1$.

There are n^n possible ways to implement the $p_n(\mathrm{id},\cdot)$ card-cyclic to random insertion shuffle since each of the n cards is removed once and reinserted in one of n positions. The number of ways that result in the permutation σ is thus $n^n p_n(\mathrm{id},\sigma)$. By "undoing" any such way, we get a one to one correspondence between the ways of going from id to σ using our original shuffle, which removes and reinserts the cards in the order $1,2,\cdots,n$, and the ways of going from σ to id using the shuffle which removes and reinserts the cards in the order $n,n-1,\cdots,1$. Thus, we conclude that

$$p_n(\mathrm{id},\sigma) = p_n^{\mathrm{id}^{\mathrm{opp}}}(\sigma,\mathrm{id}). \tag{6.1}$$

We will now calculate $p_n^{\mathrm{id}^{\mathrm{opp}}}(\sigma,\mathrm{id})$. The cards begin in the order σ. Card number n is removed first and randomly reinserted, then card number $n-1$, etc. There are n^n different ways of implementing this, and we need to know how many of these ways will result in the cards ending up in the order id. For any such way, we construct a path $\{W_j\}_{j=1}^n$ as follows. For each $j\in[n]$, let W_j denote the position in which card number j was inserted. It is clear that if the cards are to end up in the order id, then we need $W_j \le W_{j+1}$ for all j. However sometimes this is not enough and we will need instead $W_j < W_{j+1}$. To see when we only need $W_j \le W_{j+1}$ and when we need $W_j < W_{j+1}$, consider the state of the cards after the cards numbered n down to $n-j+1$ have been reinserted in such a way that they appear in increasing order from left to right. The current position of card number $n-j+1$ is by definition W_{n-j+1}. To the right of position W_{n-j+1} one finds all the cards numbered n down to $n-j+2$. If card number $n-j$ is also to the right of position W_{n-j+1}, then when it is removed and reinserted in a position which we call W_{n-j}, it will find itself to the left of card number

$n-j+1$ if and only if $W_{n-j} \le W_{n-j+1}$. However, if card number $n-j$ is to the left of position W_{n-j+1}, then when it is removed and reinserted in a position which we call W_{n-j}, it will find itself to the left of card number $n-j+1$ if and only if $W_{n-j} < W_{n-j+1}$.

Now given W_{n-j+1}, in fact we know to which side of W_{n-j+1} card number $n-j$ is to be found. Recall that $I_{n-j}(\sigma)$ is the number of inversions involving card number $n-j$ and a card with a lower number. Since none of the cards with a number lower than or equal to $n-j$ have been moved yet, it follows that these $I_{n-j}(\sigma)$ cards are to the right of card number $n-j$. Furthermore, as noted, all of the cards numbered from n down to $n-j+2$ are in positions to the right of W_{n-j+1}, and card number $n-j+1$ is in position W_{n-j+1}. From this it follows that card number $n-j$ will find itself to the left of position W_{n-j+1} if and only if $(n-j-1-I_{n-j}(\sigma))+1 \le W_{n-j+1}-1$, or equivalently if and only if $n-j-I_{n-j}(\sigma) < W_{n-j+1}$.

So we conclude that in order for the cards to end up in order id, it is necessary and sufficient that $\{W_{n-j}\}_{j=0}^{n-1}$ satisfy $W_{n-j} \le W_{n-j+1}$, with strict inequality holding if $n-j-I_{n-j}(\sigma) < W_{n-j+1}$. By induction starting with n and descending, it follows that $W_{n-j} \le n-j$, for all $j=0,\cdots,n-1$; in particular, $W_1 = 1$.

Now define $Y_j = n+1-W_{n-j+1}$, $j=1,\cdots,n$. We have $Y_j \le Y_{j+1}$. In terms of $\{Y_j\}_{j=1}^n$, in order for the cards to end up in order id, it is necessary and sufficient that $\{Y_j\}_{j=1}^n$ satisfy $Y_j < Y_{j+1}$ if $Y_j \le j + I_{n-j}(\sigma) \equiv l_j(\sigma)$. We have thus established a one-to-one correspondence between the number of ways of implementing the shuffle according to $p_n^{\mathrm{id}^{\mathrm{opp}}}(\sigma,\cdot)$ and ending up with the cards in the order id, and the number of nondecreasing $l(\sigma)$-paths of length n. The number of such paths has been denoted by $N_n(l(\sigma))$; thus we conclude that $p_n^{\mathrm{id}^{\mathrm{opp}}}(\sigma,\mathrm{id}) = \frac{N_n(l(\sigma))}{n^n}$, and by (6.1), we also have $p_n(\mathrm{id},\sigma) = \frac{N_n(l(\sigma))}{n^n}$. □

7. Proof of Theorem 6

Since we know that $N_n(l)$ is strictly monotone in l, it suffices to show that $N_n(n-1,\cdots,1) = 2^{n-1}$ and that $N_n(1,2,\cdots,n-1) = \frac{1}{n+1}\binom{2n}{n}$.

For $k \in [n]$, there is a one-to-one correspondence between paths $\{Z_i\}_{i=1}^k$ satisfying $1 \le Z_1 < Z_2 < \cdots < Z_k = n$ and solutions $(a_1, \cdots, a_k)$ with positive integral entries to $\sum_{i=1}^k a_i = n$. The correspondence is given by $a_1 = Z_1$ and $a_i = Z_i - Z_{i-1}$, for $i = 2, \cdots, k$. As is well known, the number of such solutions is $\binom{n-1}{k-1}$ [2]. Now a path $\{Y_i\}_{i=1}^n$ is a nondecreasing l-path of length n with $l = (n-1, \cdots, n-1)$ if and only if there exists a $k \in [n]$ such that $Y_j = n$ for $j \ge k$ and such that $1 \le Y_1 < \cdots < Y_k$. For any fixed k the number of such paths was just shown to be $\binom{n-1}{k-1}$. Thus $N_n(l-1, \cdots, l-1) = \sum_{k=1}^n \binom{n-1}{k-1} = 2^{n-1}$.

We claim that for $l = (1, 2, \cdots, n-1)$, there is a one-to-one correspondence between nondecreasing l-paths of length n and Dyck paths of length $2n$. Recall that a Dyck path of length $2n$ is a path $\{Z_i\}_{i=0}^{2n}$ satisfying $Z_0 = Z_{2n} = 0, Z_j \ge 0$ and $|Z_j - Z_{j-1}| = 1$, for all $j \in [2n]$. As is well known the Catalan number $C_n = \frac{1}{n+1}\binom{2n}{n}$ gives the number of such Dyck paths [12]. It remains to show the correspondence. A Dyck path can be represented as a string of $2n$ bits, n of which are labeled H and n of which are labeled T, and such that starting to count from the left, at no intermediate stage are there fewer H's than T's. Let $\{Y_i\}_{i=1}^n$ be a nondecreasing l-path of length n corresponding to $l = (1, 2, \cdots, n-1)$. Now we map this path to the Dyck path which begins with Y_1 consecutive H's, then has one T, then has $Y_2 - Y_1$ consecutive H's, then one T, then $Y_3 - Y_2$ consecutive H's, then one T, and continues in this way until it ends with $Y_n - Y_{n-1}$ consecutive H's and one T. Recalling that by definition, $Y_i \ge i$ and that Y_{i+1} is allowed to be equal to Y_i whenever $Y_i > i$, it is easy to see that this gives the appropriate one-to-one correspondence. □

Acknowledgement. The author thanks one of the referees for a meticulous and truly perspicacious report, which improved the presentation of this paper. In particular, the analysis leading from (2.3) to (2.19) was supplied by this referee. The author's original analysis of (2.3) led to a bit weaker estimate than (2.19).

References

[1] Diaconis, P., Group Representations in Probability and Statistics, Institute of Mathematical Statistics Lecture Notes—Monograph Series, 11, IMS, Hayward, CA, 1988.

[2] Feller, W. An Introduction to Probability Theory and its Applications. Vol. I, third edition, John Wiley & Sons, Inc., 1968.

[3] Goldstein, D. and Moews, D., *The identity is the most likely exchange shuffle for large n*, Aequationes Math. 65 (2003), 3-30.

[4] Mironov, I., *(Not so) random shuffles of RC4*, Advances in cryptology—CRYPTO 2002, Lecture Notes in Comput. Sci., 2442, Springer, Berlin, (2002), 304-319.

[5] Morris, B, Ning, W. and Peres, Y., *Mixing time of the card-cycle-to-random shuffle*, arXiv:1207.3406.

[6] Mossel, E., Peres, Y. and Sinclair, A., *Shuffling by semi-random transpositions*, Foundations of Computer Science, 2004. Proceedings. 45th Annual IEEE Symposium, (2004), 572 - 581.

[7] Pinsky, R. *The dead core for reaction-diffusion equations with convection and its connection with the first exit time of the related Markov diffusion process*, Nonlinear Anal. 12 (1988), 451-471.

[8] Robbins, D. P. and Bolker, E. D., *The bias of three pseudo-random shuffles*, Aequationes Math. 22 (1981), 268-292.

[9] Saloff-Coste, L. and Zúñiga, J., *Refined estimates for some basic random walks on the symmetric and alternating groups*, ALEA Lat. Am. J. Probab. Math. Stat. 4 (2008), 359-392.

[10] Schmidt, F. and Simion, R., *Card shuffling and a transformation on S_n*, Aequationes Math. 44 (1992), 11-34.

[11] Subag, E. *A lower bound for the mixing time of the random-to-random insertions shuffle*, preprint, arXiv:1112.5847

[12] Wilf, H. S., *Generatingfunctionology*, Academic Press, 1994.

Department of Mathematics, Technion—Israel Institute of Technology, Haifa, 32000, Israel

E-mail address: pinsky@math.technion.ac.il

URL: http://www.math.technion.ac.il/~pinsky/