CYCLIC TO RANDOM TRANSPOSITION SHUFFLES

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 define two cyclic to random transposition shuffles. The first one works as follows: for $j = 1, \cdots, n$, on the j-th step transpose the card that was *originally* the j-th from the left with a random card (possibly itself). The second shuffle works as follows: on the j-th step, transpose the card that is *currently* in the j-th position from the left with a random card (possibly itself). For these shuffles, for each $b \in [0,1]$, we calculate explicitly the limiting rescaled density function of $x, 0 \leq x \leq 1$, for the probability that a card with a number around bn ends up in a position around xn, and for each $x \in [0,1]$, we calculate the limiting rescaled density function of $b, 0 \leq b \leq 1$, for the probability that the card in a position around xn will be a card with a number around bn. These density functions all have a discontinuity at $x = b$, and for each of them, the infimum of the density is obtained by approaching the discontinuity from one side, and the supremum of the density is obtained by approaching the discontinuity from the other side.

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 a recent paper [4], we analyzed the bias in the *card cyclic to random insertion shuffle*: 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

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

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

cards. The novelty 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 bias in this shuffle turned out to be surprisingly high, and possessed some interesting features. We describe one of these features now, the one that is the impetus for the present article.

According to our convention, σ_j^{-1} denotes the position occupied by card number j. Let $p_n(\mathrm{id}, \cdot)$ denote the probability distribution for the above shuffle when it starts from the identity permutation. Let $b \in [0,1]$ and let $\lim_{n\to\infty} b_n = b$, with $b_n n$ being an integer in $[n]$. It was shown that the distribution function $F_b(x) \equiv \lim_{n\to\infty} p_n(\mathrm{id}, \{\sigma_{b_n n}^{-1} \leq xn\})$ for the limiting rescaled position of a card with a number around bn possesses a density $f_b(x), 0 \leq x \leq 1$, which has a jump discontinuity; moreover, as x approaches the point of discontinuity from the left, $f_b(x)$ approaches its infimum, while as x approaches the point of discontinuity from the right, $f_b(x)$ approaches its supremum. A similar phenomenon holds also for $h_x(b), 0 \leq b \leq 1$, the density for the limiting rescaled card number in a position around xn.

In the present paper we consider the above quantities for two cyclic random transposition shuffles. The first one works as follows: for $j = 1, \cdots, n$, on the j-th step transpose the card that was *originally* the j-th from the left with a random card (possibly itself). The method in this shuffle is simply the method of the above card cyclic to random insertion shuffle transferred from the context of insertions to the context of transpositions. We call this shuffle the *card cyclic to random transposition shuffle*. The second shuffle works as follows: on the j-th step, transpose the card that is *currently* in the j-th position from the left with a random card (possibly itself). We call this shuffle the *position cyclic to random transposition shuffle*.

These two shuffles are a lot more similar to one another than the above card cyclic to random insertion shuffle is to the corresponding *position cyclic to random insertion shuffle*, defined as follows: on step j, remove and randomly reinsert the card that is *currently* in the j-th position from the left. Indeed, it is easy to see that whereas by definition, every card gets removed and reinserted in the card cyclic to random insertion shuffle, in general many

cards do not get removed and reinserted at all in the position cyclic to random insertion shuffle. On the other hand, it is easy to see that in both the card cyclic to random transposition shuffle and the position cyclic to random transposition shuffle, every card will get transposed.

We will denote the probability measures on S_n corresponding respectively to the card cyclic to random transposition shuffle and the position cyclic to random transposition shuffle starting from $\sigma \in S_n$ by $p_n^{\text{card}}(\sigma, \cdot)$ and $p_n^{\text{pos}}(\sigma, \cdot)$.

Theorem 1. *i. Under $p_n^{card}(id, \cdot)$, the random variable $\sigma_{b_n n}^{-1}$, denoting the position of card number $b_n n$, has the following behavior. Assume that $\lim_{n\to\infty} b_n = b \in [0,1]$ and that $\lim_{n\to\infty} x_n = x \in [0,1]$. Then*

$$f_b^{card}(x) \equiv \lim_{n\to\infty} np_n^{card}(id, \{\sigma_{b_n n}^{-1} = x_n n\}) = \begin{cases} e^{-1+b} + e^{-x} - e^{-1-x+b}, & x < b; \\ e^{-1+b} + e^{-x}, & x > b. \end{cases}$$

ii. Under $p_n^{card}(id, \cdot)$, the random variable $\sigma_{x_n n}$, denoting the number of the card in position $x_n n$, has the following behavior. Assume that $\lim_{n\to\infty} x_n = x \in [0,1]$ and that $\lim_{n\to\infty} b_n = b \in [0,1]$. Then

$$h_x^{card}(b) \equiv \lim_{n\to\infty} np_n^{card}(id, \{\sigma_{x_n n} = b_n n\}) = \begin{cases} e^{-1+b} + e^{-x}, & b < x; \\ e^{-1+b} + e^{-x} - e^{-1-x+b}, & b > x. \end{cases}$$

Theorem 2. *i. Under $p_n^{pos}(id, \cdot)$, the random variable $\sigma_{b_n n}^{-1}$, denoting the position of card number $b_n n$, has the following behavior. Assume that $\lim_{n\to\infty} b_n = b \in [0,1]$ and that $\lim_{n\to\infty} x_n = x \in [0,1]$. Then*

$$f_b^{pos}(x) \equiv \lim_{n\to\infty} np_n^{pos}(id, \{\sigma_{b_n n}^{-1} = x_n n\}) = \begin{cases} e^{-1+x} + e^{-b}, & x < b; \\ e^{-1+x} + e^{-b} - e^{-1-b+x}, & x > b. \end{cases}$$

ii. Under $p_n^{pos}(id, \cdot)$, the random variable $\sigma_{x_n n}$, denoting the number of the card in position $x_n n$, has the following behavior. Assume that $\lim_{n\to\infty} x_n = x \in [0,1]$ and that $\lim_{n\to\infty} b_n = b \in [0,1]$. Then

$$h_x^{pos}(b) \equiv \lim_{n\to\infty} np_n^{pos}(id, \{\sigma_{x_n n} = b_n n\}) = \begin{cases} e^{-1+x} + e^{-b} - e^{-1-b+x}, & b < x; \\ e^{-1+x} + e^{-b}, & b > x. \end{cases}$$

Remark 1. Of course, part (ii) of each to the theorems follows imediately from part (i), and gives $h_x^{\text{card}}(b) = f_b^{\text{card}}(x)$ and $h_x^{\text{pos}}(b) = f_b^{\text{pos}}(x)$. Note also that it turns out that $f_b^{\text{pos}}(x) = f_x^{\text{card}}(b)$ and $h_x^{\text{pos}}(b) = h_b^{\text{card}}(x)$.

Remark 2. All four of the above densities have a discontinuity when the variable (x or b, depending on the density) is equal to the parameter (b or x). A simple calculus exercise reveals that for each of the four above densities, the supremum is approached when the variable (x or b) approaches the value of the parameter (b or x) from one one side (left or right depending on which density), and the infimum is approached when the variable approaches the value of the parameter from the other side. Thus, for both shuffles, the most likely positions for a card with a number around bn lie right next to the least likely positions, and the most likely numbers to be found in a position around xn are right next to the least likely numbers to be found in such a position. See figures 1 and 2. That is, the phenomenon noted at the beginning of this paper with regard to the card cyclic to random insertion shuffle persists with the card cyclic and position cyclic to random transposition shuffles.

Let s and t denote generically b or x, and let $f_s^*(t)$ denote generically any of the above four density functions. The supremum of f_s^* is $e^{-1+s} + e^{-s}$, and the infimum is $e^{-1+s} + e^{-s} - e^{-1}$. We have

$$\sup_{0\le s\le 1} \sup_{0\le t\le 1} f_s^*(t) = 1 + e^{-1} \approx 1.368,$$

with the supremum approached as s and t both approach 0 or 1, with one of the two variables strictly larger than the other one, the order depending on which of the four functions is considered. We have

$$\inf_{0\le s\le 1} \inf_{0\le t\le 1} f_s^*(t) = 2e^{-\frac{1}{2}} - e^{-1} \approx .845,$$

with the infimum approached as s and t both approach $\frac{1}{2}$, with one of the two variables strictly larger than the other one, the order depending on which of the four functions is considered.

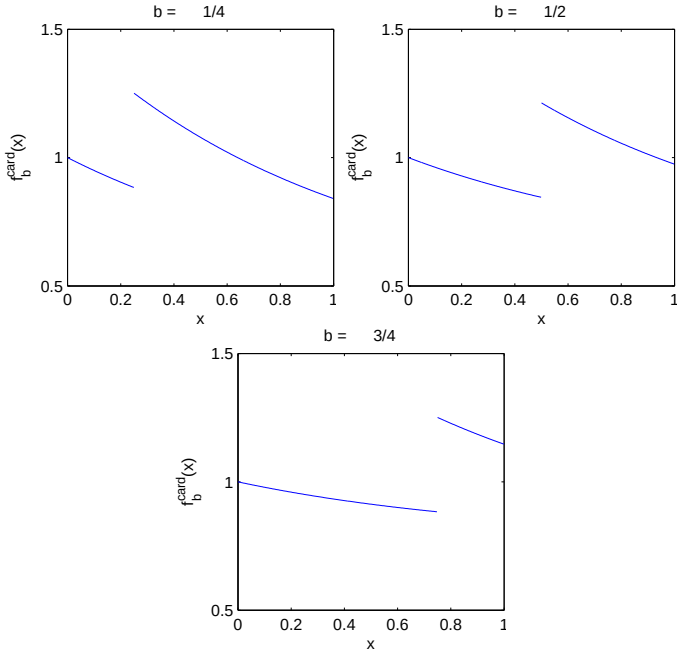

FIGURE 1. Density for limiting rescaled position of a card with a number around bn.

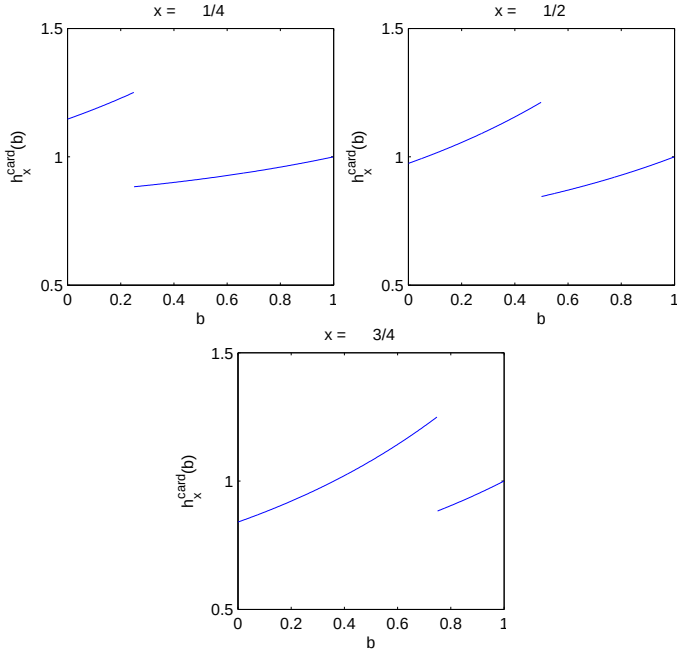

FIGURE 2. Density for limiting rescaled position of a card with a number around bn.

For the card cyclic to random transposition shuffle, let

$$E^{\text{card}}_{\text{pos}}(b) \equiv \int_0^1 x f^{\text{card}}_b(x)dx \quad \text{and} \quad E^{\text{card}}_{\text{card}}(x) \equiv \int_0^1 b h^{\text{card}}_x(b)db$$

be respectively the expected limiting rescaled position for a card with a number around bn and the expected limiting rescaled card number to be found in a position around xn, For the position cyclic to random transposition shuffle, let

$$E^{\text{pos}}_{\text{pos}}(b) \equiv \int_0^1 x f^{\text{pos}}_b(x)dx \quad \text{and} \quad E^{\text{pos}}_{\text{card}}(x) \equiv \int_0^1 b h^{\text{pos}}_x(b)db$$

be respectively the expected limiting rescaled position for a card with a number around bn and the expected limiting rescaled card number to be found in a position around xn.

Direct calculations give the following corollary.

Corollary 1. *i.*

$$E^{card}_{pos}(s) = E^{pos}_{card}(s) = 1 - \frac{1}{2}e^{-1+s} - (1+s)e^{-1}.$$

The maximum of this function occurs at $s = \log 2 \approx .693$ with the value about .519, and the minimum of this function occurs at $s = 0$ with value about .448.

ii.

$$E^{card}_{card}(s) = E^{pos}_{pos}(s) = \frac{1}{2}e^{-s} + se^{-1}.$$

The maximum of this function occurs at $s = 1$ with the value about .552, and the minimum of this function occurs at $s = 1 - \log 2 \approx .307$ with value about .481.

In the case of the card cyclic to random insertion shuffle, the density $f_b(x)$ degenerated when $b \to 0$ to include a δ-mass at $x = 0$ of weight e^{-1}. Using this as a starting point, we were able to show that the total variation distance between the distribution $p_n(\text{id}, \cdot)$ and the uniform distribution 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

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

In the cases at hand, we don't know whether the total variation distance between $p_n^{\text{card}}(\text{id}, \cdot)$ and the uniform distribution or between $p_n^{\text{pos}}(\text{id}, \cdot)$ and the uniform distribution goes to 1. Let U_n denote the uniform distribution on S_n. The above results just allow us to obtain the following result.

Corollary 2. *Let $p_n^*(id, \cdot)$ be generic notation for either $p_n^{pos}(id, \cdot)$ or $p_n^{card}(id, \cdot)$. Then*

$$\lim_{n\to\infty} ||p_n^*(id, \cdot) - U_n||_{TV} \geq \sup_{b\in[0,1]} \frac{1}{2} \int_0^1 |f_b^{card}(x) - 1| dx = ?. \tag{1.1}$$

As was the case with the card cyclic to random insertion shuffle, the card cyclic to random transposition shuffle does not seem to have been studied before. On the other hand, the position cyclic to random transposition shuffle has been studied. From the point of view of mixing times, it was studied in [2] and [3], where it was shown that as $n \to \infty$, the number of such shuffles needed to approach equilibrium is on the order $\log n$. More in the spirit of this paper, the papers [5], [6] and [1] all studied various aspects of the distribution $p_n^{\text{pos}}(\text{id}, \cdot)$, such as the limiting probability of a derangement occurring, or the limiting expected number of fixed points. In [5] it was shown that $p_n^{\text{pos}}(\text{id}, \sigma) \geq \frac{2^{n-1}}{n^n}$, for all $\sigma \in S_n$, and that the inequality is an equality when σ is the permutation which cycles every card to the right. In [1] it was also shown that for $n \geq 18$, but not for $3 \leq n \leq 17$, the identity permutation has the highest probability; furthermore, as $n \to \infty$, $p_n^{\text{pos}}(\text{id}, \text{id}) \sim \frac{\frac{1}{\sqrt{2}} n^{\frac{n}{2}} e^{-\frac{n}{2}+\sqrt{n}-\frac{1}{4}}}{n^n}$ ([5, p. 276], [1]). By comparison, we note that in [4] we showed that for the card cyclic to random insertion shuffle, one has the sharp inequalities $\frac{2^{n-1}}{n^n} \leq p_n(\text{id}, \cdot) \leq \frac{C_n}{n^n}$, where $C_n = \frac{1}{n+1}\binom{2n}{n} \sim \frac{1}{\sqrt{\pi} n^{\frac{3}{2}}} \frac{4^n}{n^n}$ is the n-th Catalan number. The results in [5], [6], and [1] do not at all allow one to determine whether or not $\lim_{n\to\infty} ||p_n^{\text{pos}}(\text{id}, \cdot) - U_n||_{\text{TV}} = 1$. We pose this as a question:

Question: Does $\lim_{n\to\infty} ||p_n^{\text{pos}}(\text{id}, \cdot) - U_n||_{\text{TV}} = 1$?

Theorem 1 is proved in section 2 and Theorem 2 is proved in section 3.

2. Proof of Theorem 1

Since $p_n^{\text{card}}(\text{id}, \{\sigma_j^{-1} = a\}) = p_n^{\text{card}}(\text{id}, \{\sigma_a = j\})$, part (ii) of the theorem follows immediately from part (i). We now prove part (i).

For $a, j \in [n]$ with $a \neq j$, we consider $p_n^{\text{card}}(\text{id}, \{\sigma_j^{-1} = a\})$, the probability that card number j ends up in position a. The shuffle has n steps, each of which is constituted by a transposition. One way for $\{\sigma_j^{-1} = a\}$ to occur is for card number j to move to position a on the j-th step of the shuffle, and then for it never to move again. The probability of this occurring is $\frac{1}{n}(1 - \frac{1}{n})^{n-j}$. The reader should convince himself that if on the other hand, card number j moves to position a on the j-th step of the shuffle, but is involved later on in another transposition, then it cannot end up in position a. Another way for $\{\sigma_j^{-1} = a\}$ to occur is if $j < a$, card number a is not moved before step a, on step a card number a is transposed with card number j, and then card number j is never transposed again. The probability of this is $\frac{1}{n}(1 - \frac{1}{n})^{n-1}$, if $j < a$. If one the other hand, card number j is transposed again after step a, then it can not end up in position a.

Assuming now that card number j is not moved to position a on the j-step or on the a-th step, we consider how else one can end up with the event $\{\sigma_j^{-1} = a\}$. The reader should convince himself of the following facts. (Remember that all the following statements are being made under the assumption that card number j does not move to position a on step j or on step a.) If card number a gets transposed before the a-th step, then card number j cannot end up in position a. (For example, say card number a gets transposed for the first time on the i-th step, with $i < a$. If card number i was not transposed before the i-th step, then on the i-th step, card number a was transposed with card number i. So now after the i-th step, card number i is in position a. On every later step k, card number k will be transposed with a random card. Since we are assuming that card number j was not moved to position a on the j-th step, there is no way for card number j to end up in position a. Similarly, if card number i was transposed before step i, say at step l, and card number l was not transposed before step l, then on

the i-th step, card number a was transposed with card number l. And the same logic as above shows that card number j cannot end up in position a.)

If card number a gets transposed for the first time at step a, and gets transposed with a card whose number is less than or equal to a, but not equal to j, then card number j cannot end up in position a. (The reasoning is similar to the above reasoning.)

If card number a gets transposed for the first time at step a, and gets transposed with a card whose number l is greater than a, but then card number l gets transposed between step a and step l, then for reasons similar to the above, card number j cannot end up in position a.

However, if number card a gets transposed for the first time at step a, and gets transposed with a card whose number l is greater than a, and then card number l is not transposed between step a and step l, then there is still a chance for card j to end up in position a. One way would be if $l > j$ and if on step l, card number l is transposed with card number j, and then after step l, card number j is never transposed again (this last requirement is possible because $l > j$). Another way would be for card number l to get transposed on step l with card number m with $m > l$ and $m > j$, then for card number m not to get transposed between step l and step m, then for card number m to be transposed with card number j on step m, and then for card number j not to be transposed again after step m (this last requirement is possible because $m > j$). Continuing to argue in this vein, we arrive at the following formula.

Let F_k denote the first step on which card number k is transposed. Of course, from the definition of the shuffle one has $F_k \leq k$. Let T_k^i denote the last step strictly before the i-th step on which card number k was transposed. If there is no such step then define $T_k^i = \infty$. We will use the generic P when considering probabilities related to the random variables F_k and T_k^i. Then

we have

(2.1)

$$p_n^{\text{card}}(\text{id}, \{\sigma_j^{-1} = a\}) = \frac{1}{n}(1-\frac{1}{n})^{n-j} + \frac{1}{n}(1-\frac{1}{n})^{n-1}1_{j<a} + \sum_{m=1}^{n-a} \sum_{a \equiv i_0 < i_1 < \cdots < i_m \leq n; i_m > j} P(F_a = a) \left(\prod_{l=1}^{m} P(T_{i_l}^{i_l} = i_{l-1}) \right) P(T_j^{n+1} = i_m).$$

We have $P(F_a = a) = (1-\frac{1}{n})^{a-1}$, $P(T_{i_l}^{i_l} = i_{l-1}) = \frac{1}{n}(1-\frac{1}{n})^{i_l - i_{l-1}-1}$ and $P(T_j^{n+1} = i_m) = \frac{1}{n}(1-\frac{1}{n})^{n-i_m}$, with this last equality holding because $i_m > j$. Substituting this in (2.1) gives

$$p_n^{\text{card}}(\text{id}, \{\sigma_j^{-1} = a\}) = \frac{1}{n}(1-\frac{1}{n})^{n-j} + \frac{1}{n}(1-\frac{1}{n})^{n-1}1_{j<a} + \sum_{m=1}^{n-a} \sum_{a \equiv i_0 < i_1 < \cdots < i_m \leq n; i_m > j} (1-\frac{1}{n})^{n-m-1}(\frac{1}{n})^{m+1}. \tag{2.2}$$

If $m > j-a$, then the restriction $i_m > j$ on the inner sum above is superfluous and we have

$$\sum_{a \equiv i_0 < i_1 < \cdots < i_m \leq n; i_m > j} 1 = \binom{n-a}{m}.$$

If $m \leq j-a$, then we have

$$\sum_{a \equiv i_0 < i_1 < \cdots < i_m \leq n; i_m > j} 1 = \sum_{i_m = j+1}^{n} \binom{i_m - 1 - a}{m-1}.$$

Using this with (2.2) gives

$$\begin{aligned} p_n^{\text{card}}(\text{id}, \{\sigma_j^{-1} = a\}) &= \frac{1}{n}(1-\frac{1}{n})^{n-j} + +\frac{1}{n}(1-\frac{1}{n})^{n-1}1_{j<a} + \\ &\sum_{m=(j-a)^+ +1}^{n-a} (1-\frac{1}{n})^{n-m-1}(\frac{1}{n})^{m+1}\binom{n-a}{m} + \\ &\sum_{m=1}^{(j-a)^+} (1-\frac{1}{n})^{n-m-1}(\frac{1}{n})^{m+1} \left(\sum_{r=j+1}^{n} \binom{r-1-a}{m-1} \right), \end{aligned} \tag{2.3}$$

where any summation whose lower limit is greater than its upper limit is understood to vanish.

Let $X_{\mathrm{Bin}(N,q)}$ denote a binomial random variable with parameters N and q. We have

(2.4)
$$\sum_{m=(j-a)^+ +1}^{n-a} (1-\frac{1}{n})^{n-m-1}(\frac{1}{n})^{m+1}\binom{n-a}{m} = (1-\frac{1}{n})^{a-1}\frac{1}{n}P(X_{\mathrm{Bin}(n-a,\frac{1}{n})} \geq (j-a)^+ +1).$$

Similarly, for $r \in \{j+1, \cdots, n\}$, we have

$$\sum_{m=1}^{(j-a)^+} (1-\frac{1}{n})^{n-m-1}(\frac{1}{n})^{m+1}\binom{r-1-a}{m-1} = \frac{1}{n^2}(1-\frac{1}{n})^{n-r+a-1}P(X_{\mathrm{Bin}(r-1-a,\frac{1}{n})} \leq (j-a)^+ - 1). \tag{2.5}$$

Now let $a = x_n n$ and let $j = b_n n$, with $\lim_{n\to\infty} x_n = x$, $\lim_{n\to\infty} b_n = b$, and $b \neq x$. We conclude from (2.4) that

(2.6)
$$\lim_{n\to\infty} n \sum_{m=(b_n n - x_n n)^+ +1}^{n-x_n n} (1-\frac{1}{n})^{n-m-1}(\frac{1}{n})^{m+1}\binom{n-x_n n}{m} = \begin{cases} e^{-x}(1-e^{-1+x}), \text{ if } x > b; \\ 0, \text{ if } x < b. \end{cases}$$

For all $r \in \{b_n n + 1, \cdots, n\}$, we have

$$\lim_{n\to\infty} P(X_{\mathrm{Bin}(r-1-x_n n,\frac{1}{n})} \leq (b_n n - x_n n)^+ - 1) = 1, \text{ if } x < b. \tag{2.7}$$

It then follows from (2.5) and (2.7) that

(2.8)
$$\lim_{n\to\infty} n \sum_{m=1}^{(b_n n - x_n n)^+} (1-\frac{1}{n})^{n-m-1}(\frac{1}{n})^{m+1}\left(\sum_{r=b_n n+1}^{n}\binom{r-1-x_n n}{m-1}\right) =$$
$$\lim_{n\to\infty} \sum_{r=b_n n+1}^{n} \frac{1}{n}(1-\frac{1}{n})^{n-r+x_n n-1} = e^{-1-x}\int_b^1 e^x dx = e^{-x} - e^{-1-x+b}, \text{ if } x < b.$$

If $x > b$, then the left hand side of (2.8) is identically 0 for large n.

It now follows from (2.3), (2.6) and (2.8) that

$$\lim_{n\to\infty} np_n^{\mathrm{card}}(\mathrm{id}, \{\sigma_{b_n n}^{-1} = x_n n\}) = \begin{cases} e^{-1+b} + e^{-x}, \ x > b; \\ e^{-1+b} + e^{-x} - e^{-1-x+b}, \ x < b. \end{cases} \tag{2.9}$$

□

3. Proof of Theorem 2

Since $p_n^{\text{pos}}(\text{id}, \{\sigma_j^{-1} = a\}) = p_n^{\text{pos}}(\text{id}, \{\sigma_a = j\})$, part (ii) of the theorem follows immediately from part (i). We now prove part (i).

The analysis here is similar to that in the proof of Theorem 1 so we will be less thorough here with the explanations. For $a, j \in [n]$ with $a \neq j$, we consider $p_n^{\text{pos}}(\text{id}, \{\sigma_j^{-1} = a\})$, the probability that card number j ends up in position a. The shuffle has n steps, each of which is constituted by a transposition. One way for $\{\sigma_j^{-1} = a\}$ to occur is for card number j to be moved to position a on the a-th step and then for card number j never to move again. The probability of this is $\frac{1}{n}(1 - \frac{1}{n})^{n-a}$. Another way for $\{\sigma_j^{-1} = a\}$ to occur is if $a < j$, card number j does not move before the j-th step of the shuffle, on the j-th step it moves to position a, and then it never moves again after the j-th step. The probability of this is $\frac{1}{n}(1 - \frac{1}{n})^{n-1}$, if $a < j$. On the other hand, if card number j moves to position a on the a-th step and then moves again later on, it cannot end up in position a. Similarly, if $a < j$, and card number j moves to position a on the j-th step of the shuffle, and then moves again later on, it cannot end up in position a.

Assuming now that card number j is not moved to position a on the j-step or on the a-th step, we consider how else one can end up with the event $\{\sigma_j^{-1} = a\}$. By reasoning similar to that in the proof of Theorem 1, the only other way for this event to occur is if there exists an $m \geq 1$ and numbers $\{i_l\}_{l=1}^m$ satisfying $j < i_1 < \cdots < i_m \leq n$, with $i_m > a$, such that card number j does not move until step j, at step j it is moved to position i_1, and then after that it moves again only at steps i_l, $l = 1, \cdots, m$, with it moving at step i_l, $l = 1, \cdots, m-1$, to position i_{l+1}, and with it moving at step i_m to position a. The probability of the above occurring for a particular choice of m and $\{i_l\}_{l=1}^m$ is

$$(1 - \frac{1}{n})^{j-1}\frac{1}{n}(1 - \frac{1}{n})^{i_1-j-1} \times \cdots \times \frac{1}{n}(1 - \frac{1}{n})^{i_m-i_{m-1}-1}\frac{1}{n}(1 - \frac{1}{n})^{n-i_m} =$$
$$(1 - \frac{1}{n})^{n-m-1}(\frac{1}{n})^{m+1}.$$

If $m > a - j$, then the restriction above that $i_m > a$ is superfluous and we have

$$\sum_{j<i_1<\cdots<i_m\le n; i_m>a} 1 = \binom{n-j}{m}.$$

If $m \le a - j$, then we have

$$\sum_{j<i_1<\cdots<i_m\le n; i_m>a} 1 = \sum_{i_m=a+1}^{n} \binom{i_m - 1 - j}{m-1}.$$

From the above analysis we conclude that

$$\begin{aligned} p_n^{\mathrm{pos}}(\mathrm{id}, \{\sigma_j^{-1} = a\}) &= \frac{1}{n}(1-\frac{1}{n})^{n-a} + \frac{1}{n}(1-\frac{1}{n})^{n-1} 1_{a<j} + \\ &\sum_{m=(a-j)^+ +1}^{n-j} (1-\frac{1}{n})^{n-m-1}(\frac{1}{n})^{m+1}\binom{n-j}{m} + \\ &\sum_{m=1}^{(a-j)^+} (1-\frac{1}{n})^{n-m-1}(\frac{1}{n})^{m+1}\left(\sum_{r=a+1}^{n}\binom{r-1-j}{m-1}\right), \end{aligned} \tag{3.1}$$

where any summation whose lower limit is greater than its upper limit is understood to vanish. Noting that the right hand side of (3.1) is the right hand side of (2.3) with the roles of a and j switched, part (i) of the theorem follows from part (i) of Theorem 1. □.

References

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

[2] Mironov, I., *(Not so) random shuffles of RC4*, Advances in cryptologyCRYPTO 2002, 304319, Lecture Notes in Comput. Sci., 2442, Springer, Berlin, (2002), 304-319.

[3] 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.

[4] Pinsky, R., *Probabilistic and Combinatorial Aspects of the Card-Cyclic to Random Insertion Shuffle*, submitted.

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

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

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/