NOTES ON THE DIACONIS–FULMAN BIJECTION

MARK WILDON

This note presents a bijective proof due to Diaconis and Fulman [2] of Theorem 3.1 below. The case $b = 2$ of this theorem relates riffle shuffles to the ranking permutations of random binary numbers. We define these objects in §1 and §2 below. The theorem is stated in §3 and proved in §6 using the preliminary results on the dagger and star re-ordering maps in §4 and §5. No originality is claimed.

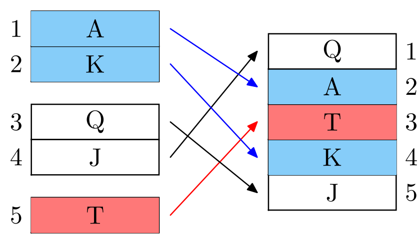
1. Shuffles

We use position permutations to represent shuffles, thus if $\tau(i) = j$ then the card in position i is moved to position j. As in [2] we multiply permutations from right to left. We note that if τ is a shuffle performed on a pack of cards numbered from 1 (at the top) to r (at the bottom) then $\tau^{-1}(j) = i$ if and only if card i ends in place j. Therefore the one-line form of τ^{-1} encodes the new pack order.

Fix $b \in \mathbf{N}$ with $b \geq 2$. Besides the meaning in the definition below, b will be the base in which we represent natural numbers.

Definition 1.1. A *b-riffle shuffle* of r cards is a permutation $\tau \in \mathrm{Sym}_r$ obtained by choosing a set composition $\big(J(1), \ldots, J(b)\big)$ of $\{1, \ldots, r\}$ uniformly at random, and then setting $\tau(c_m + i) = J(m)_i$ where $c_m = |J(1)| + \cdots + |J(m-1)|$ and $J(m)_i$ is the ith smallest element of $J(m)$.

For example, a 2-riffle shuffle τ is obtained by choosing a subset $J \subseteq \{1, \ldots, r\}$ uniformly at random; if $J = \{j_1, \ldots, j_c\}$ and $\{1, \ldots, r\} \backslash J = \{k_1, \ldots, k_d\}$, where $j_1 < \ldots < j_c$ and $k_1 < \ldots < k_d$, then $\tau(i) = j_i$ for $1 \leq i \leq c$ and $\tau(a + i) = k_i$ for $1 \leq i \leq d$. In this shuffle the top c cards end in positions $j_1, \ldots, j_c$ and the bottom d cards end in positions $k_1, \ldots, k_d$. The one-line form is therefore $j_1 \ldots j_c k_1 \ldots k_d$. The diagram below the 3-riffle shuffle 24153 for $(\{2,4\}, \{1,5\}, \{3\})$ performed on the five honour cards in a suit.



Date: July 26 2019, some corrections made 1 January 2025.

As expected, $\tau^{-1} = 31524$ gives the new pack order. (Thus our riffle shuffles are the inverses of those in [2].)

The remainder of this section is not logically essential.

GSR-model for riffle shuffles. An alternative model for shuffling is due to Gilbert and Shannon, and, independently, Reeds (see references in [1]). In this model the deck is cut into b piles, so that pile 1 consisting of some of the cards at the top of the deck, and pile b consisting of some of the cards at the bottom of the deck, and the probability that the piles have sizes $r_1, \ldots, r_b$ is the multinomial $\binom{r}{r_1,\ldots,r_b}/b^r$. (Thus some piles may be empty.) A shuffled deck is then constructed from the top down, so that if at some step the piles have sizes $s_1, \ldots, s_b \in \mathbf{N}_0$, the probability the next card comes from the top of pile m is $s_m/(s_1 + \cdots + s_b)$. (Except for the top-down rebuilding order, this corresponds to dropping cards with probability proportion to the weight of the piles they lie in.) Let $(p_\tau)_{\tau \in \mathrm{Sym}_r}$ be the probability distribution of GSR-shuffles.

Example 1.2. Let $b = 3$. The 3-riffle shuffle 231 (written in one-line form) is obtained from the set compositions

$$\big(\{2\},\{3\},\{1\}\big), \big(\{2,3\},\{1\},\varnothing\big), \big(\{2,3\},\varnothing,\{1\}\big), \big(\varnothing,\{2,3\},\{1\}\big),$$

and so has probability $\frac{4}{27}$. In the GSR-model, starting with the deck AKQ and ending with QAK (from top-to-bottom), it is obtained from the cuts leaving piles $(\mathrm{A},\mathrm{K},\mathrm{Q})$, $(\mathrm{AK},\mathrm{Q},\varnothing)$, $(\mathrm{AK},\varnothing,\mathrm{Q})$, $(\varnothing,\mathrm{AK},\mathrm{Q})$, necessarily by rebuilding in the order $(\mathrm{Q},\mathrm{A},\mathrm{K})$. The contributions to p_{231} are $\frac{1}{3^3}\binom{3}{1,1,1}\frac{1}{3} \times \frac{1}{2} = \frac{1}{3^3}$ and (in each remaining case) $\frac{1}{3^3}\binom{3}{2,1}\frac{1}{3} = \frac{1}{3^3}$, hence $p_{231} = \frac{4}{27}$.

More generally, we have the following result, proved as Lemma 1 and Theorem 3 in [1]. Recall that a permutation $\tau \in \mathrm{Sym}_r$ has a *descent* in position i if and only if $\tau(i) > \tau(i+1)$. We denote the number of descents of τ by $d(\tau)$.

Lemma 1.3.
(i) *Choosing b-riffle shuffles of r-cards uniformly at random, the probability of choosing $\tau \in \mathrm{Sym}_r$ is p_τ.*
(ii) *We have $p_\tau = \binom{r+b-d(\tau)-1}{r}/b^r$.*

Proof. Given a set composition $\big(J(1),\ldots,J(b)\big)$ corresponding to the b-riffle shuffle τ there is a corresponding GSR-shuffle, in which the deck is cut into piles of sizes $|J(1)|,\ldots,|J(b)|$ and the deck is rebuilt so that the jth card comes from pile m if and only if $\tau^{-1}(j) \in J(m)$. Using the notation of Definition 1.1, the ith card from pile m, which began in position $c_m + i$ of the original deck, finishes in position j, where $\tau^{-1}(j) = c_m + i$. Hence $\tau(c_m + i) = J(m)_i$, as required. The product of the probabilities from the second phase of the GSR-model is in every case $\frac{J(1)!\ldots J(b)!}{r!} = \binom{r}{|J(1)|,\ldots,|J(r)|}^{-1}$, so the contribution to p_τ is $1/b^r$. This proves (i). (Note it also shows that in the GSR-model, the effect that some partitions are more likely than others is cancelled out by the probabilities in the dropping phase.) For (ii), take the set composition of $\{1,\ldots,r\}$ into $d(\tau)$ sets that corresponds to τ, and observe that there are $\binom{r+b-d(\tau)-1}{b-d(\tau)-1}$ ways to refine it (by dividing the one-line form of τ in $b-d(\tau)-1$ places) into a set composition into b parts still corresponding to τ. $\square$

The main application of Theorem 3.1 concerns descents of inverse riffle-shuffles and their compositions. This statistic has very different properties. For example, a non-identity 2-riffle shuffle $\tau \in \mathrm{Sym}_{2s}$ has a unique descent, whereas τ^{-1} may have any number of descents between 1 and s. The maximum is achieved (uniquely) by the 2-riffle shuffle $24\ldots(2s)13\ldots(2s-1)$, with inverse $(s+1)1(s+2)2\ldots(2s)s$.

2. Ranking permutations and the dagger map

We define the *ranking permutation* π of an r tuple $(x_1,\ldots,x_r)$ of elements from a totally ordered set by $\pi(i)=j$ if x_i is the jth smallest element in the tuple. Ties are broken by the rule that if $i<i'$ and $x_i=x_{i'}$ then x_i has lower rank than $x_{i'}$. Less algorithmically, an equivalent definition of π is

$$\pi(i)=\bigl|\{k : 1\le k\le r, x_k<x_i \text{ or both } x_k=x_i \text{ and } k<i\}\bigr|.$$

We say $\pi(i)$ is the *rank* of element i of $(x_1,\ldots,x_r)$, or more informally, that $\pi(i)$ is the rank of x_i. (Strictly speaking the latter is ambiguous when x_i appears multiple times.)

Example 2.1.

(1) The ranking permutation of $(1,0,2,1,0)$ is 31542 in one-line form and the ranking permutation of $(2,3,1,4)$ is simply 2314.
(2) More generally, if τ is a permutation of $\{1,\ldots,r\}$ then, since x has rank x in any tuple of distinct elements from an initial segment of the natural numbers, the ranking permutation of $\bigl(\tau(1),\ldots,\tau(r)\bigr)$ is τ.
(3) The set composition $\bigl(\{2,4\},\{1,5\},\{3\}\bigr)$ corresponds, by recording the part containing each entry, to the 5-tuple $(2,1,3,1,2)$. The ranking permutation of this tuple is 31524 and its inverse is the 3-riffle shuffle 24153 corresponding to $\bigl(\{2,4\},\{1,5\},\{3\}\bigr)$.

The third example motivates the following lemma.

Lemma 2.2. *The ranking permutation of r numbers, chosen uniformly at random from $\{0,1,\ldots,b-1\}$, has the same distribution as the inverse of a uniform-at-random b-riffle shuffle of r cards.*

Proof. Suppose that the numbers are $x_1,\ldots,x_r$ and that $x_j=m$ if and only if $j\in J(m)\subseteq\{1,\ldots,m\}$. Let π be the ranking permutation of $(x_1,\ldots,x_r)$.

Suppose that x_j is the ith smallest element of $J(m)$. Then counting the lower ranked elements lying in $J(1), \ldots, J(m-1)$, we see that $\pi(j) = |J(1)| + \cdots + |J(m-1)| + i$. Therefore π^{-1} is the b-riffle shuffle corresponding to the set composition $\big(J(1), \ldots, J(m)\big)$. $\square$

3. Diaconis–Fulman Theorem

This theorem relates iterated inverse riffle shuffles to the ranking permutations of r numbers, lying in $\{0, \ldots, b^k - 1\}$, under addition in base b. We use bold letters for such numbers, and roman letters for their base b digits. Ranking permutations were defined in §2 above.

Theorem 3.1 (Diaconis–Fulman)**.** *Let k, $r \in \mathbf{N}$. Let $\vartheta_1, \ldots, \vartheta_k \in \mathrm{Sym}_r$ be inverse b-riffle shuffles, chosen uniformly at random. Let $\mathbf{x}_1, \ldots, \mathbf{x}_r \in \{0, \ldots, b^k - 1\}$ be chosen uniformly at random. For $1 \le p \le k$ let*

- *$\tau_p \in \mathrm{Sym}_r$ be the composition $\vartheta_p \ldots \vartheta_1$.*
- *$\pi_p \in \mathrm{Sym}_r$ be the ranking permutation of $(\mathbf{x}_1 \bmod b^p, \ldots, \mathbf{x}_r \bmod b^p)$.*

The joint distributions of $(\tau_k, \ldots, \tau_1)$ and $(\pi_k, \ldots, \pi_1)$ agree.

While this theorem is not stated in [2], it follows from the key Lemma 3.5 in this paper. This may be the intended content of the remark following the proof of Theorem 3.1 in [2]. However there is some ambiguity about whether this remark is a claim on the distribution of τ_k, or on the joint distribution of $\tau_1, \ldots, \tau_k$. Note that the case $k = 1$ is Lemma 2.2.

Example 3.2. The 2-riffle shuffles in Sym_3 are $123, 132, 213, 231, 312$. Following the Gilbert–Shannon–Reeds model, the identity has probability $1/2$ and the other four each have probability $1/8$. For example, to obtain 132 we must split the deck as 12, 3, and reassemble (from the top-down) in the order 1, 3, 2; this has probability $\frac{1}{2^3}\binom{3}{1}\frac{2}{3}\frac{1}{2} = \frac{1}{8}$. (This example is atypical in that a shuffle and its inverse have the same probability.) The first matrix below, with rows labelled by τ_1 and columns by τ_2, shows the number of pairs $(\vartheta_2, \vartheta_1)$ of inverse 2-riffle shuffles of three cards such that $\vartheta_1 = \tau_1$ and $\vartheta_2\vartheta_1 = \tau_2$. The second matrix is the transition matrix of the Markov chain on Sym_3 with generators the inverse 2-riffle shuffles (chosen with the appropriate probabilities).

$$\begin{array}{c} 123 \\ 132 \\ 213 \\ 231 \\ 312 \\ 321 \end{array} \begin{pmatrix} 16 & 4 & 4 & 4 & 4 & 0 \\ 1 & 4 & 1 & 1 & 0 & 1 \\ 1 & 1 & 4 & 0 & 1 & 1 \\ 1 & 1 & 0 & 4 & 1 & 1 \\ 1 & 0 & 1 & 1 & 4 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \qquad \frac{1}{8}\begin{pmatrix} 4 & 1 & 1 & 1 & 1 & 0 \\ 1 & 4 & 1 & 1 & 0 & 1 \\ 1 & 1 & 4 & 0 & 1 & 1 \\ 1 & 1 & 0 & 4 & 1 & 1 \\ 1 & 0 & 1 & 1 & 4 & 1 \\ 0 & 1 & 1 & 1 & 1 & 4 \end{pmatrix}$$

As predicted by Theorem 3.1, the first matrix also records the number of $\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3 \in \{0, 1, 2, 3\}$ such that $(\mathbf{x}_1 \bmod 2, \mathbf{x}_2 \bmod 2, \mathbf{x}_3 \bmod 2)$ has ranking permutation τ_1 and $(\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3)$ has ranking permutation τ_2. For example, the entry 1 in row 132 and column 213 comes uniquely from $(\vartheta_1, \vartheta_2) = (132, 231)$ and from $(\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3) = (10, 01, 10)$.

Application to carries. The aim of [2] is the following application. Let $\mathbf{x}_1, \ldots, \mathbf{x}_r \in \{0, \ldots, b^k - 1\}$ be chosen uniformly at random and let $\mathbf{s}_1, \ldots, \mathbf{s}_r$ be their partial sums, defined by $\mathbf{s}_i = \mathbf{x}_1 + \cdots + \mathbf{x}_i$ for $1 \le i \le r$. A new carry is created going into position $p+1$ on addition (in base b) of $\mathbf{x}_i$ to $\mathbf{s}_{i-1}$ if and only if

$$\mathbf{s}_i \bmod b^p < \mathbf{s}_{i-1} \bmod b^p.$$

Thus the total carry C_p into position $p+1$ is the number of descents of the ranking permutation of $(\mathbf{s}_1 \bmod b^p, \ldots, \mathbf{s}_r \bmod b^p)$. Denote this permutation by π'_p. The map $(\mathbf{x}_1, \ldots, \mathbf{x}_r) \mapsto (\mathbf{s}_1, \ldots, \mathbf{s}_r)$ is a self-bijection of the set of r-tuples of elements of $\{0, \ldots, b^k - 1\}$. Therefore the distributions of $(\pi'_k, \ldots, \pi'_1)$ and $(\pi_k, \ldots, \pi_1)$ agree and Theorem 3.1 implies that

$$\mathbf{P}[C_k = d_k, \ldots, C_1 = d_1] = \mathbf{P}[d(\tau_k) = d_k, \ldots, d(\tau_1) = d_1)]$$

for all $d_k, \ldots, d_1 \in \mathbf{N}_0$.

It is a small calculation to see that the maximum possible carry is $r-1$ (independently of b); this is obvious in the riffle-shuffle interpretation. Since the carry going into position $p+1$ depends only on the carry going into position p (and the numbers we add), but not on earlier carries, the tuple $(C_1, \ldots, C_k)$ is a Markov chain on $\{0, \ldots, r-1\}$. This is far from obvious in the shuffles interpretation. (As noted in this context in [3, §2], the image of a Markov chain under a function is not usually a Markov chain.)

Example 3.3. The transition matrices for the carries process when $b = 2$ and $r \in \{2, 3, 4, 5\}$ are shown below.

$$\frac{1}{4}\begin{pmatrix} 3 & 1 \\ 1 & 3 \end{pmatrix}, \; \frac{1}{8}\begin{pmatrix} 4 & 1 & 0 \\ 4 & 6 & 4 \\ 0 & 1 & 4 \end{pmatrix}, \; \frac{1}{16}\begin{pmatrix} 5 & 1 & 0 & 0 \\ 10 & 10 & 5 & 1 \\ 1 & 5 & 10 & 10 \\ 0 & 0 & 1 & 5 \end{pmatrix}, \; \frac{1}{32}\begin{pmatrix} 6 & 1 & 0 & 0 & 0 \\ 20 & 15 & 6 & 1 & 0 \\ 6 & 15 & 20 & 15 & 0 \\ 0 & 1 & 6 & 15 & 20 \\ 0 & 0 & 0 & 1 & 6 \end{pmatrix}$$

These are instances of Holte's *amazing matrices*: see [4] and MathOverflow question 258284. When we add r bits, of which exactly w are 1, with an initial carry of c, the new carry is c' where $c + w \in \{2c', 2c' + 1\}$. Therefore the amazing matrices for $b = 2$ may be defined by

$$P(r)_{c'c} = \frac{1}{2^r}\left(\binom{r}{w} + \binom{r}{w+1}\right) \quad \text{where } w = 2c' - c.$$

One of the amazing properties is that the eigenvalues are $1, 1/2, \ldots, 1/2^{r-1}$. Explicit eigenvectors are found in [4]; the eigenvector for 1, giving the invariant distribution of the Markov chain, is $(\frac{1}{r!}\left\langle {r \atop 0} \right\rangle, \frac{1}{r!}\left\langle {r \atop 1} \right\rangle, \ldots, \frac{1}{r!}\left\langle {r \atop r-1} \right\rangle)$. Here the Eulerian number $\left\langle {r \atop c} \right\rangle$ is the number of permutations of $\{1, \ldots, r\}$ having exactly c descents.

Application to shuffles. Another corollary of Theorem 3.1 is as follows.

Corollary 3.4. *Let ϕ and ϑ be random b-shuffles of r cards. Then $\phi\vartheta$ is distributed as a random b^2-shuffle of r cards.*

Proof. The ranking permutation of r numbers in $\{0, 1, \ldots, b^2 - 1\}$ chosen uniformly at random does not depend on whether these numbers are regarded as single digit numbers in base b^2 (giving a random b^2-shuffle, by Lemma 2.2, or the special case $k = 1$ of Theorem 3.1), or as double digit numbers in base b (giving the distribution of $\phi\vartheta$ by Theorem 3.1). □

The more general result behind this is that if ϕ is a random a-shuffle and ϑ is a random b-shuffle then $\phi\vartheta$ is distributed as a random ab-shuffle. This was proved by Holte [4] (see remark after Theorem 3) in the setting of carries, and has an easier proof in the setting of shuffles given in [2] (see (3) on page 3).

4. The dagger map

In this section we define the main building block for the star map in [2]. Let $(x_1, \ldots, x_r)$ and $(y_1, \ldots, y_r)$ be r-tuples from totally ordered finite sets X and Y, respectively. Write $x_i y_j$ for the element $(x_i, y_j) \in X \times Y$ and order $X \times Y$ lexicographically, i.e. first by X then by Y. Let π be the ranking permutation for $(y_1, \ldots, y_r)$. Define

$$(x_1 y_1, \ldots, x_r y_r)^\dagger = (x_{\pi(1)} y_1, \ldots, x_{\pi(r)} y_r).$$

For example, if $X = Y = \{0, 1, 2\}$ with the usual total order then since $(1, 2, 0, 1)$ has ranking permutation 2413 in one-line form, we have

$$(x_1 1, x_2 2, x_3 1, x_4 0)^\dagger = (x_2 1, x_4 2, x_3 0, x_1 1).$$

It is easily seen that the dagger map is a bijection.

Proposition 4.1. *Let X and Y be totally ordered finite sets. Let $(x_1, \ldots, x_r) \in X^r$ and $(y_1, \ldots, y_r) \in Y^r$. Let π be the ranking permutation of $(y_1, \ldots, y_r)$. Let τ be the ranking permutation of $(x_1, \ldots, x_r)$ and let $\tau^\dagger$ be the ranking permutation of $(x_{\pi(1)} y_1, \ldots, x_{\pi(r)} y_r)$. Then $\tau^\dagger = \tau \circ \pi$.*

To motivate the proof we consider two special cases. First suppose that $(x_1, \ldots, x_r)$ has distinct entries. In this case, the ranking permutations of $(x_{\pi(1)} y_1, \ldots, x_{\pi(r)} y_r)$ and $(x_{\pi(1)}, \ldots, x_{\pi(r)})$ agree, since we need compare only on the first parts. The latter is $\tau \circ \pi$. Secondly, suppose that all the x_i are equal. Then τ is the identity and the ranking permutations of $(x_{\pi(1)} y_1, \ldots, x_{\pi(r)} y_r)$ and $(y_1, \ldots, y_r)$ agree. So we have $\tau^\dagger = \pi$, as required. It is worth noting that the second case shows that the ranking permutation of $(x_{\pi(1)}, \ldots, x_{\pi(r)})$ is, in general, not $\tau \circ \pi$. The dagger map may be regarded as correcting for this.

Proof of Proposition 4.1. We compare ranks of the elements in the tuples $(x_{\pi(1)}, \ldots, x_{\pi(r)})$ and $(x_{\pi(1)}y_1, \ldots, x_{\pi(r)}y_r)$.

Let $i < i'$. Suppose that $x_{\pi(i)} < x_{\pi(i')}$. Then $\tau(\pi(i)) < \tau(\pi(i'))$ and, since we need to compare $x_{\pi(i)}y_i$ and $x_{\pi(i')}y_{i'}$ only on their first parts, $\tau^\dagger(i) < \tau^\dagger(i')$. Similarly if $x_{\pi(i)} > x_{\pi(i')}$ then $\tau(\pi(i)) > \tau(\pi(i'))$ and $\tau^\dagger(i) > \tau^\dagger(i')$.

Now suppose that $x_{\pi(i_1)} = \ldots = x_{\pi(i_c)} = x$ where $\pi(i_1) < \ldots < \pi(i_c)$. Let s be the number of $x_{\pi(i)}y_i$ such that $x_{\pi(i)} < x$. Observe that:

> *the rank, in $\{1, \ldots, c\}$ of the entry y_{i_a} in position a of the tuple $(y_{i_1}, \ldots, y_{i_c})$ is the rank, again in $\{1, \ldots, c\}$, of the entry $\pi(i_a)$ in position a of the tuple $(\pi(i_1), \ldots, \pi(i_c))$.*

In $(x_{\pi(1)}y_1, \ldots, x_{\pi(r)y_r})$, the ranks of the entries $xy_{i_1}, \ldots, xy_{i_c}$ are, as a set, $s+1, \ldots, s+c$, and the rank of the entry xy_{i_c} in position i_a is s plus the rank of y_{i_a} in the tuple $(y_{i_1}, \ldots, y_{i_c})$. In $(x_1, \ldots, x_r)$, the ranks of the entries (all equal to x) in positions $\pi(i_1), \ldots, \pi(i_c)$ are, as a set $s+1, \ldots, s+c$, and the rank of the entry $x_{\pi(i_c)}$ in position $\pi(i_c)$ is s plus the rank of $\pi(i_c)$ in $(\pi(i_1), \ldots, \pi(i_c))$. These agree, by the observation.

It follows that $\pi \circ \tau = \pi^\dagger$. $\square$

It is tempting to short-cut the second part of the proof by claiming it reduces to the case, considered before the proof, where *all* the x_i are equal. This feels convincing, but after some thought, I am not sure it should be. Proposition 4.1 is a special case of Lemma 3.5 in [2], where the proof again is quite demanding on the reader's intuition.

5. The star map

Let $X(1), \ldots, X(k)$ be totally ordered finite sets. We use bold letters to denote elements of $X(k) \times \cdots X(1)$; thus $\mathbf{x}$ denotes the k-tuple $(\mathbf{x}(k), \ldots, \mathbf{x}(1))$. Extending the notational convention used for $X \times Y$ in the previous section, we write $\mathbf{x}(p) \ldots \mathbf{x}(1)$ for the final p elements of this tuple. Given an r-tuple $(\mathbf{x}_1, \ldots, \mathbf{x}_r)$ of elements of $X(k) \times \cdots \times X(1)$, define

$$\big(\mathbf{y}_1(1), \ldots, \mathbf{y}_r(1)\big) = \big(\mathbf{x}_1(1), \ldots, \mathbf{x}_r(1)\big),$$

and for each $p \in \{2, \ldots, k\}$, define $\mathbf{y}_1(p), \ldots, \mathbf{y}_r(p)$ by

$$\big(\mathbf{y}_1(p) \ldots \mathbf{y}_1(2)\mathbf{y}_1(1), \ \ldots, \ \mathbf{y}_r(p) \ldots \mathbf{y}_r(2)\mathbf{y}_r(1)\big) = \big(\mathbf{x}_1(p)\mathbf{w}_1, \ldots, \mathbf{x}_r(p)\mathbf{w}_r\big)^\dagger$$

where, for each $i \in \{1, \ldots, r\}$, we set $\mathbf{w}_i = y_i(p-1) \ldots y_i(1)$, thought of as an element of the totally ordered set $X(p-1) \times \cdots \times X(1)$. The *star map* is then defined by $(\mathbf{x}_1, \ldots, \mathbf{x}_r)^\star = (\mathbf{y}_1, \ldots, \mathbf{y}_r)$.

Example 5.1. Let $X(3) = X(2) = X(1) = \{0, 1\}$. Then

$$\big(01, 11, 01, 10\big)^\star = \big(01, 11, 01, 11\big)^\dagger = (11, 01, 11, 00)$$

since the ranking permutation of $(1,1,1,0)$ is 2341, so we reorder $x = (0,1,0,1)$ as $(x_{\pi(1)}, x_{\pi(2)}, x_{\pi(3)}, x_{\pi(4)}) = (x_2, x_3, x_4, x_1) = (1,0,1,0)$. Hence

$$\bigl(101, 011, 001, 110\bigr)^\star = (1(11), 0(01), 1(11), 1(00))^\dagger = (011, 001, 111, 100).$$

Lemma 5.2. *Let* $(\mathbf{x}_1, \ldots, \mathbf{x}_r)^\star = (\mathbf{y}_1, \ldots, \mathbf{y}_r)$. *Let* $p \in \{1, \ldots, k\}$. *Let* $\mathbf{z}'$ *denote the* p*-tuple obtained from* $\mathbf{z} \in X(k) \times \cdots \times X(1)$ *by taking the final* p *entries. Then*

$$(\mathbf{x}'_1, \ldots, \mathbf{x}'_r)^\star = (\mathbf{y}'_1, \ldots, \mathbf{y}'_r).$$

Proof. This is obvious from the iterative definition of the star map. □

6. Proof of Theorem 3.1

For convenience we repeat the statement of the theorem below.

Theorem 6.3. *Let* $k,\ r \in \mathbf{N}$. *Let* $\vartheta_1, \ldots, \vartheta_k \in \mathrm{Sym}_r$ *be inverse* b*-riffle shuffles, chosen uniformly at random. Let* $\mathbf{x}_1, \ldots, \mathbf{x}_r \in \{0, \ldots, b^k - 1\}$ *be chosen uniformly at random. For* $1 \le p \le k$ *let*

- $\tau_p \in \mathrm{Sym}_r$ *be the composition* $\vartheta_p \ldots \vartheta_1$.
- $\pi_p \in \mathrm{Sym}_r$ *be the ranking permutation of* $(\mathbf{x}_1 \bmod b^p, \ldots, \mathbf{x}_r \bmod b^p)$.

The joint distributions of $(\tau_k, \ldots, \tau_1)$ *and* $(\pi_k, \ldots, \pi_1)$ *agree.*

For $\mathbf{x} \in \{0, \ldots, b^k - 1\}$, we identify $\mathbf{x}$ with the tuple $\mathbf{x}(k) \ldots \mathbf{x}(2)\mathbf{x}(1) \in \{0, \ldots, b-1\}^k$ of its base b digits, defined by

$$\mathbf{x} = \mathbf{x}(k)b^{k-1} + \cdots + \mathbf{x}(2)b + \mathbf{x}(1).$$

Observe that if $\mathbf{x} \in \mathbf{N}_0$ then $\mathbf{x} \bmod b^p$ is $\mathbf{x}(p)b^{p-1} + \cdots + \mathbf{x}(2)b + \mathbf{x}(1)$, which may be identified with $\mathbf{x}(p) \ldots \mathbf{x}(1)$.

Proof of Theorem 3.1. Since the dagger map is a bijection, so is the star map. Hence there exist unique $\mathbf{y}_1, \ldots, \mathbf{y}_r \in \{0, \ldots, b^k - 1\}$ such that $(\mathbf{y}_1, \ldots, \mathbf{y}_r)^\star = (\mathbf{x}_1, \ldots, \mathbf{x}_r)$.

We show, by induction on p, that the joint distributions of $(\tau_p, \ldots, \tau_1)$ and $(\pi_p, \ldots, \pi_1)$ agree. When $p = 1$ this is Lemma 2.2. Let $p \ge 2$ and let ϑ_p be the ranking permutation of $\bigl(\mathbf{y}_1(p), \ldots, \mathbf{y}_r(p)\bigr)$. This is consistent with the statement of the theorem because, by Lemma 2.2, ϑ_p is a uniform-at-random inverse b-riffle shuffle. Let $\mathbf{w}_i = \mathbf{x}_i \bmod p^{b-1}$ for each i. By Lemma 5.2 we have

$$\begin{aligned}(\mathbf{x}_1 \bmod b^p, \ldots, \mathbf{x}_r \bmod b^p) &= (\mathbf{y}_1 \bmod b^p, \ldots, \mathbf{y}_r \bmod b^p)^\star \\ &= (\mathbf{y}_1(p)\mathbf{w}_1, \ldots, \mathbf{y}_r(p)\mathbf{w}_r)^\dagger.\end{aligned}$$

The ranking permutation of the left-hand side is, by definition, π_p, and, again by definition, the ranking permutation of $(\mathbf{w}_1, \ldots, \mathbf{w}_r)$ is π_{p-1}. Hence, by Proposition 4.1, we have $\pi_p = \vartheta_p \circ \pi_{p-1}$. The theorem follows. □

References

[1] Dave Bayer and Persi Diaconis, *Trailing the dovetail shuffle to its lair*, Ann. Appl. Probab. **2** (1992), no. 2, 294–313.

[2] Persi Diaconis and Jason Fulman, *Carries, shuffling, and an amazing matrix*, Amer. Math. Monthly **116** (2009), no. 9, 788–803.

[3] ———, *Carries, shuffling, and symmetric functions*, Adv. in Appl. Math. **43** (2009), no. 2, 176–196.

[4] John M. Holte, *Carries, combinatorics, and an amazing matrix*, Amer. Math. Monthly **104** (1997), no. 2, 138–149.