Carries, Shuffling, and an Amazing Matrix

Persi Diaconis and Jason Fulman

1. INTRODUCTION. In a wonderful article in this MONTHLY, John Holte [22] found fascinating mathematics in the usual process of "carries" when adding integers. His article reminded us of the mathematics of shuffling cards. This connection is developed below.

Consider adding two 40-digit binary numbers (the top row, in italics, comprises the carries):

1	*01110*	*01000*	*00001*	*00111*	*10111*	*00000*	*00111*	*1110*
	10111	00110	00000	10011	11011	10001	00011	11010
	10011	10101	11110	10001	01000	11010	11001	01111
1	01010	11011	11111	00101	00100	01011	11101	01001

For this example, $19/40 = 47.5\%$ of the columns have a carry of 1. Holte shows that if the binary digits are chosen at random, uniformly, in the limit 50% of all the carries are zero. This holds no matter what the base. More generally, if one adds n integers (base b) that are produced by choosing their digits uniformly at random in $\{0, 1, \ldots, b-1\}$, the sequence of carries $\kappa_0 = 0, \kappa_1, \kappa_2, \ldots$ is a Markov chain taking values in $\{0, 1, 2, \ldots, n-1\}$. The Markov property holds because to compute the amount carried to the next column, one only needs to know the carry and numbers in the current column: the past does not matter. We let $P(i, j) = \mathbb{P}(\kappa' = j \mid \kappa = i)$ denote an entry of the transition matrix between successive carries κ and κ'. Holte found the following:

(H1) For $0 \le i, j \le n-1$,

$$P(i, j) = \frac{1}{b^n} \sum_{r=0}^{j-\lfloor i/b \rfloor} (-1)^r \binom{n+1}{r} \binom{n-1-i+(j+1-r)b}{n}.$$

For example, for $n = 2$ and all b,

$$(P(i, j)) = \frac{1}{2b} \begin{pmatrix} b+1 & b-1 \\ b-1 & b+1 \end{pmatrix},$$

and for $n = 3$ and all b,

$$(P(i, j)) = \frac{1}{6b^2} \begin{pmatrix} b^2+3b+2 & 4b^2-4 & b^2-3b+2 \\ b^2-1 & 4b^2+2 & b^2-1 \\ b^2-3b+2 & 4b^2-4 & b^2+3b+2 \end{pmatrix}.$$

In the special case when $b = 2$, for any n, Holte derives the simpler expression

$$P(i, j) = \frac{1}{2^n} \cdot \binom{n+1}{2j-i+1} \qquad 0 \le i, j \le n-1.$$

doi:10.4169/000298909X474864

The matrices of **(H1)** are the "amazing matrices" of Holte's title, and we also denote them by P_b. Among many things, Holte shows:

(H2) The matrix P_b has stationary vector π (left eigenvector with eigenvalue 1) independent of the base b:

$$\pi(j) = \frac{A(n, j)}{n!},$$

where $A(n, j)$ is an Eulerian number. The $n!$ in the denominator is to make the entries of the left eigenvector sum to 1.

The Eulerian number $A(n, j)$ may be defined as the number of permutations in the symmetric group S_n with j descents. Recall that $\sigma \in S_n$ has a descent at position i if $\sigma(i+1) < \sigma(i)$. So **5 1 3 2 4** has two descents. Note that we write permutations as sequences, where the ith number in the sequence denotes $\sigma(i)$.

When $n = 2$, $A(2, 0) = A(2, 1) = 1$, and thus $\pi(0) = \pi(1) = 1/2$ is the limiting frequency of carries when two long integers are added. When $n = 3$, $A(3, 0) = 1$, $A(3, 1) = 4$, and $A(3, 2) = 1$, giving $\pi(0) = 1/6$, $\pi(1) = 2/3$, and $\pi(2) = 1/6$.

We mention that Eulerian numbers make many mathematical appearances, e.g., in the theory of sorting [**26**] and in juggling sequences [**10**]. For further background on their properties, the reader can consult [**12**].

Holte further establishes the remarkable:

(H3) The matrix P_b has eigenvalues $1, 1/b, 1/b^2, \ldots, 1/b^{n-1}$ with explicitly computable left and right eigenvectors independent of b.

(H4) $P_a P_b = P_{ab}$ for all real a and b.

When we saw properties **(H2)**, **(H3)**, and **(H4)**, we hollered "Wait, this is all about shuffling cards!" Readers who know us may well think, "For these two guys, everything is about shuffling cards." While there is some truth to these thoughts, we justify our claim in the next section. Following this we show how the connection between carries and shuffling contributes to each subject. The rate of convergence of the Markov chain **(H1)** to the stationary distribution π is given in Section 4: the argument shows that the matrix P_b is totally positive of order 2. Finally, we show how the same matrix occurs in taking sections of generating functions [**9**], discuss carries for multiplication, and describe another "amazing matrix."

Our developments do not exhaust the material in Holte's article, which we enthusiastically recommend. A "higher math" perspective on arithmetic carries as cocycles [**23**] suggests many further projects. We have tried to keep the presentation elementary, and mention the (more technical) companion paper [**15**] which analyzes the carries chain using symmetric function theory and gives analogs of our main results for other Coxeter groups.

2. SHUFFLING CARDS. How many times should a deck of n cards be riffle shuffled to thoroughly mix it? For an introduction to this subject, see [**2, 27**]. The main theoretical developments are in [**5, 16**] with further developments in [**18, 19**]. A survey of the many connections and developments is in [**14**]. The basic shuffling mechanism was suggested by [**20**]. It gives a realistic mathematical model for the usual method of riffle shuffling n cards:

- Cut off C cards with probability $\binom{n}{C}/2^n$, $0 \le C \le n$.
- Shuffle the two parts of the deck according to the following rule: if at some stage there are A cards in one part and B cards in the other part, drop the next card from

the bottom of the first part with probability $A/(A+B)$ and from the bottom of the second part with probability $B/(A+B)$.

- Continue until all cards are dropped.

Let $Q(\sigma)$ be the probability of generating the permutation σ after one shuffle, starting from the identity, and let $Q^h(\sigma)$ denote the corresponding quantity after h successive shuffles. Repeated shuffling is modeled by convolution:

$$Q^2(\sigma) = \sum_\eta Q(\eta)Q(\sigma\eta^{-1}), \quad Q^h(\sigma) = \sum_\eta Q^{h-1}(\eta)Q(\sigma\eta^{-1}). \tag{1}$$

Thus to be at σ after two shuffles, the first shuffle goes to some permutation η and the second must be to $\sigma\eta^{-1}$. The uniform distribution is $U(\sigma) = 1/n!$. Standard theory shows that

$$Q^h(\sigma) \to U(\sigma) \quad \text{as } h \to \infty. \tag{2}$$

The reference [**5**] gives useful rates for the convergence in (2), showing that for $h = (3/2)\log_2 n + c$ with c fixed,

$$\frac{1}{2}\sum_\sigma |Q^h(\sigma) - U(\sigma)| \to 1 - 2\Phi\left(\frac{-2^{-c}}{4\sqrt{3}}\right) \quad \text{with } \Phi(x) = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{x} e^{-t^2/2}\,dt$$

as $n \to \infty$. Roughly stated, it takes $h = (3/2)\log_2 n + c$ shuffles to get 2^{-c} close to random; when $n = 52$ and $h = 7$, the above distance to uniform is about 0.3 and tends to zero exponentially thereafter.

To explain the connection with carries, it is useful to have a geometric description of shuffling. Consider dropping n points uniformly at random into $[0, 1)$. Label these points in order $x_{(1)} \le x_{(2)} \cdots \le x_{(n)}$. The baker's transformation $x \mapsto 2x \bmod 1$ maps $[0, 1)$ into itself and permutes the points. Let σ be the induced permutation. As shown in [**5**], the chance of σ is exactly $Q(\sigma)$. A natural generalization of this shuffling scheme to "b-shuffles" is induced from $x \mapsto bx \bmod 1$ with b fixed in $\{1, 2, 3, \dots\}$. Thus ordinary riffle shuffles are 2-shuffles and a 3-shuffle results from dividing the deck into three piles and dropping cards sequentially from the bottom of each pile with probability proportional to packet size.

Let $Q_b(\sigma)$ be the probability of σ after a b-shuffle. Letting $*$ be the convolution operator used in equation (1), one can show [**5**] from the geometric description that

$$Q_a * Q_b = Q_{ab}. \tag{3}$$

The key is to check that the points $ax_{(1)} \bmod 1, ax_{(2)} \bmod 1, \dots, ax_{(n)} \bmod 1$ have the same distribution as n uniform points in $[0, 1)$, so the b-shuffle can be applied to these points without having to reposition them at random in $[0, 1)$. Then (3) follows since $b(ax_{(i)} \bmod 1) \bmod 1 = abx_{(i)} \bmod 1$.

The physical model of shuffling described at the start of this section is Q_2 in this notation and we see that $Q_2^h = Q_{2^h}$. Thus to study repeated shuffles, we need only understand a single b-shuffle. A main result of [**5**] is a simple formula:

$$Q_b(\sigma) = \frac{\binom{n+b-r}{n}}{b^n}. \tag{4}$$

Here $r = r(\sigma) = 1 + \#\{\text{descents in } \sigma^{-1}\}$.

In addition to the similarities between **(H4)** and (3), [**5**] and [**21**] proved that the eigenvalues of the Markov chain induced by Q_b are also $1, 1/b, 1/b^2, \ldots, 1/b^{n-1}$ (though here $1/b^i$ occurs with multiplicity equal to the number of permutations in S_n with $n - i$ cycles instead of with multiplicity 1). This and the appearance of descents convinced us that there must be an intimate connection between carries and shuffling. The main result of this article (proved in Section 3) makes this precise.

Theorem 2.1. *The number of descents in successive b-shuffles of n cards forms a Markov chain on* $\{0, 1, \ldots, n-1\}$ *with transition matrix* $(P(i, j))$ *of* **(H1)**.

3. BIJECTIVE METHODS. First we describe some notation to be used throughout. The number of descents of a permutation τ is denoted by $d(\tau)$. Label the columns of the n numbers to be added base b by $C_1, C_2, C_3, \ldots$, where C_1 is the rightmost column.

The main purpose of this section is to give a bijective proof of the following theorem, which implies Theorem 2.1.

Theorem 3.1. *Let* κ_j *denote the amount carried from column* j *to column* $j + 1$ *when* n *m-digit base-b numbers are added, and the digits are chosen uniformly and independently from* $\{0, 1, \cdots, b-1\}$. *Let* τ_j *be the permutation obtained after the first* j *steps of a sequence of m b-shuffles of n cards, started at the identity. Then*

$$\mathbb{P}(\kappa_1 = i_1, \ldots, \kappa_m = i_m) = \mathbb{P}(d(\tau_1) = i_1, \ldots, d(\tau_m) = i_m)$$

for all values of $i_1, \ldots, i_m$.

In preparation for the proof of Theorem 3.1, some definitions and lemmas are needed. To begin, note that κ_j is determined by the last j columns $C_j \cdots C_1$. Given a length-n list of j-digit base-b numbers, one says that the list has a carry at position i if the addition of the $(i + 1)$st number on the list to the sum of the first i numbers on the list increases the amount that would be carried to the $(j + 1)$st column (it might seem more natural to say that the carry is at position $i + 1$, but our convention will be useful). For example the following list of 3-digit base-3 numbers:

$$\begin{array}{ccc} 0 & 1 & 2 \\ 0 & 1 & 2 \\ 1 & 1 & 2 \\ 1 & 1 & 1 \\ 2 & 1 & 2 \\ 1 & 2 & 1 \end{array}$$

has a carry at positions 3 and 4. Indeed $012 + 012 = 101$ which doesn't create a carry. Adding 112 gives 220 which still doesn't create a carry. Adding 111 gives 101 with a carry, so there is a carry at position 3. Adding 212 gives 020 with a carry, so there is a carry at position 4. Finally adding 121 gives 211, which doesn't create a carry.

Note that when there is a carry at position i, the carry is 1. This observation yields the following lemma.

Lemma 3.2. *Let* $\kappa(C_j \cdots C_1)$ *denote the number of positions* i *such that when the base-b numbers given by* $C_j \cdots C_1$ *are added, there is a carry at position* i. *Then* $\kappa(C_j \cdots C_1) = \kappa_j$.

Given a length-n list of j-digit base-b numbers, one says that the list has a descent at position i if the $(i+1)$st number on the list is smaller than the ith number on the list. For example the following list of 3-digit base-3 numbers:

$$\begin{matrix} 0 & 1 & 2 \\ 1 & 0 & 1 \\ 2 & 2 & 0 \\ 1 & 0 & 1 \\ 0 & 2 & 0 \\ 2 & 1 & 1 \end{matrix}$$

has a descent at position 3 since 220 is greater than 101, and a descent at position 4 since 101 is greater than 020.

For what follows we use a bijection, which we call the bar map, on length-n lists of j-digit base-b numbers. Letting $a_1, \ldots, a_n$ denote the n numbers on this list, the bar map may be described as

$$(a_1, \ldots, a_n) \mapsto (a_1, a_1 + a_2, a_1 + a_2 + a_3, \ldots, a_1 + \cdots + a_n)$$

where addition is mod b^j. For example,

$$C_3C_2C_1 = \begin{matrix} 0 & 1 & 2 \\ 0 & 1 & 2 \\ 1 & 1 & 2 \\ 1 & 1 & 1 \\ 2 & 1 & 2 \\ 1 & 2 & 1 \end{matrix} \mapsto \overline{C_3C_2C_1} = \begin{matrix} 0 & 1 & 2 \\ 1 & 0 & 1 \\ 2 & 2 & 0 \\ 1 & 0 & 1 \\ 0 & 2 & 0 \\ 2 & 1 & 1 \end{matrix}.$$

Indeed $012 + 012 = 101$ giving the second line of $\overline{C_3C_2C_1}$. Then $101 + 112 = 220$ giving the third line, and $220 + 111 = 101$ (retaining only the last 3 digits), giving the fourth line, etc. One can easily invert the bar map, so it is a bijection.

Remark. The bar map was shown to us by Jim Fill with the suggestion that it would lead to a bijective proof of Theorem 3.1. Our analytic proof is recorded in [**15**].

The following lemma is immediate from the above definitions.

Lemma 3.3. *$\overline{C_j \cdots C_1}$ has a descent at position i if and only if $C_j \cdots C_1$ has a carry at position i.*

Given a length-n list of j-digit base-b numbers, we define an associated permutation π by labeling the n numbers from smallest to largest (considering the higher-up number to be smaller in case of ties). For example with $n = 6$, $j = 2$, and $b = 3$, one would have

$$\pi = \pi \begin{pmatrix} 1 & 2 \\ 2 & 1 \\ 1 & 0 \\ 0 & 1 \\ 0 & 0 \\ 2 & 1 \end{pmatrix} = \begin{matrix} 4 \\ 5 \\ 3 \\ 2 \\ 1 \\ 6 \end{matrix},$$

since 00 is the smallest, followed by 01, 10, 12, then the uppermost copy of 21, and finally the lowermost copy of 21. Note that, by the convention we use for writing permutations, this means that $\pi(1) = 4$, $\pi(2) = 5$, etc. We mention that this construction appears in the theory of inverse riffle shuffling [5].

Lemma 3.4. *$\overline{C_j \cdots C_1}$ has a descent at position i if and only if the associated permutation $\pi(\overline{C_j \cdots C_1})$ has a descent at position i.*

Proof. This is immediate from the definition of π. ∎

To proceed we define a second bijection, called the star map, on length-n lists of j-digit base-b numbers. As above, it is useful to think of such a list as a sequence of j length-n column vectors with entries in $0, 1, \ldots, b-1$. The star map sends column vectors $A_j \cdots A_1$ to $(A_j \cdots A_1)^*$ defined as follows. The rightmost column of $(A_j \cdots A_1)^*$ is A_1. The second column in $(A_j \cdots A_1)^*$ is obtained by putting the entries of A_2 in the order specified by the permutation corresponding to the rightmost column of $(A_j \cdots A_1)^*$ (which is A_1); i.e., if $\pi = \pi(A_1)$, what gets put in position j is the $\pi(j)$th entry of A_2. Then the third column in $(A_j \cdots A_1)^*$ is obtained by putting the entries of A_3 in the order specified by the permutation corresponding to the two rightmost columns of $(A_j \cdots A_1)^*$, and so on.

For example,

$$A_3A_2A_1 = \begin{matrix} 1 & 2 & 2 \\ 1 & 2 & 1 \\ 2 & 0 & 0 \\ 0 & 0 & 1 \\ 2 & 1 & 0 \\ 0 & 1 & 1 \end{matrix} \mapsto (A_3A_2A_1)^* = \begin{matrix} 0 & 1 & 2 \\ 1 & 0 & 1 \\ 2 & 2 & 0 \\ 1 & 0 & 1 \\ 0 & 2 & 0 \\ 2 & 1 & 1 \end{matrix}.$$

Indeed, the rightmost column of $(A_3A_2A_1)^*$ is A_1. The second column of $(A_3A_2A_1)^*$ is obtained by taking the entries of A_2 (namely 2, 2, 0, 0, 1, 1) and putting the first 2 next to the smallest element of A_1 (so the highest 0), then the second 2 next to the 2nd smallest element (so the second 0), then the first 0 next to the 3rd smallest element (so the highest 1), then the second 0 next to the 4th smallest element (so the second 1), then the first 1 next to the 5th smallest element (so the third 1), and finally the second 1 next to the 6th smallest element (so the only 2), giving

$$\begin{matrix} 1 & 2 \\ 0 & 1 \\ 2 & 0 \\ 0 & 1 \\ 2 & 0 \\ 1 & 1 \end{matrix}.$$

Then the third column of $(A_3A_2A_1)^*$ is obtained by taking the entries of A_3 (namely 1, 1, 2, 0, 2, 0) and putting the first 1 next to the smallest pair (so the highest 01), then putting the second 1 next to the 2nd smallest pair (so the second 01), then the first 2 next to the third smallest pair 11, then the first 0 next to the fourth smallest pair 12, then the second 2 next to the fifth smallest pair (the highest 20), and finally the second 0 next to the sixth smallest pair (the second 20).

The star map is straightforward to invert (we leave this as an exercise to the reader), so it is a bijection.

The crucial property of the star map is given by the following lemma, the $j = 2$ case of which is essentially equivalent to the "$A^B\&B$" formula in [**27**, Section 9.4].

Lemma 3.5.

$$\pi(A_j)\cdots\pi(A_1) = \pi[(A_j\cdots A_1)^*],$$

where the product on the left is the usual multiplication of permutations.

As an illustration,

$$A_3A_2A_1 = \begin{matrix} 1 & 2 & 2 \\ 1 & 2 & 1 \\ 2 & 0 & 0 \\ 0 & 0 & 1 \\ 2 & 1 & 0 \\ 0 & 1 & 1 \end{matrix}$$

yields the permutations

$\pi(A_3)$	$\pi(A_2)$	$\pi(A_1)$
3	5	6
4	6	3
5	1	1
1	2	4
6	3	2
2	4	5

Also as calculated above,

$$(A_3A_2A_1)^* = \begin{matrix} 0 & 1 & 2 \\ 1 & 0 & 1 \\ 2 & 2 & 0 \\ 1 & 0 & 1 \\ 0 & 2 & 0 \\ 2 & 1 & 1 \end{matrix}$$

which yields the permutations

$\pi[(A_3A_2A_1)^*]$	$\pi[(A_2A_1)^*]$	$\pi[(A_1)^*]$
1	4	6
3	1	3
6	5	1
4	2	4
2	6	2
5	3	5

We thus have the equalities $\pi[(A_1^*)] = \pi(A_1)$, $\pi[(A_2A_1)^*] = \pi(A_2)\pi(A_1)$, and $\pi[(A_3A_2A_1)^*] = \pi(A_3)\pi(A_2)\pi(A_1)$, and Lemma 3.5 gives that this happens in general.

Proof of Lemma 3.5. This is clear for $j = 1$, so consider $j = 2$. Then the claim is perhaps easiest to see using the theory of inverse riffle shuffles. Namely, given a column

of n 1-digit base-b numbers, label cards $1, \ldots, n$ with these numbers, then bring the cards labeled 0 to the top (cards higher up remaining higher up), then bring the cards labeled 1 just beneath them, and so on. For instance,

Card	*Label*		*Card*	*Label*
1	2		3	0
2	1		5	0
3	0	$\mapsto$	2	1
4	1		4	1
5	0		6	1
6	1		1	2

Note that the third column of the table represents $\pi(A_1)^{-1}$. Now repeat this process, using the column

$$\begin{matrix} 2 \\ 2 \\ 0 \\ 0 \\ 1 \\ 1 \end{matrix}$$

to label the cards, placing the labels just to the left of the digit already on each card. A moment's thought shows that this is equivalent to a single process in which one labels the cards with pairs from $(A_2A_1)^*$. Thus $\pi[(A_2A_1)^*]^{-1} = \pi(A_1)^{-1}\pi(A_2)^{-1}$, so that $\pi[(A_2A_1)^*] = \pi(A_2)\pi(A_1)$. The reader desiring further discussion for the case of two columns is referred to Section 9.4 of the expository paper [**27**]. The argument for $j \geq 3$ is identical: just use the observation that iterating the procedure three times is equivalent to a single process in which one labels the cards with triples from $(A_3A_2A_1)^*$. ■

With the above preparations in hand, Theorem 3.1 can be proved.

Proof of Theorem 3.1. To begin, note that

$$\begin{aligned} \kappa_1 = i_1, \ldots, \kappa_m = i_m &\Leftrightarrow \kappa(C_j \cdots C_1) = i_j \ (1 \leq j \leq m) \\ &\Leftrightarrow d(\overline{C_j \cdots C_1}) = i_j \ (1 \leq j \leq m) \\ &\Leftrightarrow d(\pi(\overline{C_j \cdots C_1})) = i_j \ (1 \leq j \leq m). \end{aligned}$$

The first step used Lemma 3.2, the second step used Lemma 3.3, and the third step used Lemma 3.4.

Let $A_m \cdots A_1 = (\overline{C_m \cdots C_1})^{-*}$, where $-*$ denotes the inverse of the star map. Then $A_j \cdots A_1 = (\overline{C_j \cdots C_1})^{-*}$ for all $1 \leq j \leq m$, and Lemma 3.5 implies that

$$d[\pi(A_j) \cdots \pi(A_1)] = d(\pi[(A_j \cdots A_1)^*]) = d[\pi(\overline{C_j \cdots C_1})],$$

so the above equivalences can be extended to

$$\Leftrightarrow d[\pi(A_j) \cdots \pi(A_1)] = i_j \ (1 \leq j \leq m).$$

Now note that if the entries of $C_m \cdots C_1$ are chosen independently from the uniform distribution on $\{0, 1, \ldots, b-1\}$, then the same is true of $A_m \cdots A_1$ since the bar and

star maps are both bijections. Note that each $\pi(A_i)$ has the distribution of a permutation after a b-shuffle, so one may take τ_j to be the product $\pi(A_j)\cdots\pi(A_1)$, and the theorem is proved. ∎

Remark and example. The above construction may appear complicated, but we mention that the star map (though useful in the proof) is not needed in order to go from the numbers being added to the τ's. Indeed, from the proof of Theorem 3.1 one sees that the τ_j's can be defined by $\tau_j = \pi(\overline{C_j \cdots C_1})$. Thus in the running example,

$$C_3C_2C_1 = \begin{matrix} 0&1&2\\ 0&1&2\\ 1&1&2\\ 1&1&1\\ 2&1&2\\ 1&2&1 \end{matrix} \mapsto \overline{C_3C_2C_1} = \begin{matrix} 0&1&2\\ 1&0&1\\ 2&2&0\\ 1&0&1\\ 0&2&0\\ 2&1&1 \end{matrix} \mapsto \begin{matrix} \tau_3&\tau_2&\tau_1\\ 1&4&6\\ 3&1&3\\ 6&5&1\\ 4&2&4\\ 2&6&2\\ 5&3&5 \end{matrix}.$$

Observe that $\kappa_1 = 3, \kappa_2 = 3$, and $\kappa_3 = 2$, and that $d(\tau_1) = 3, d(\tau_2) = 3$, and $d(\tau_3) = 2$, as claimed.

As a corollary of Theorem 3.1, we deduce that the descent process after riffle shuffles is Markov (usually, a function of a Markov chain is not Markov).

Corollary 3.6. *Let a Markov chain on the symmetric group begin at the identity and proceed by successive independent b-shuffles. Then $d(\pi)$, the number of descents, forms a Markov chain.*

Proof. This follows from Theorem 3.1 and the fact that the carries process is Markov. ∎

4. APPLICATIONS TO THE CARRIES PROCESS. As in previous sections, let κ_j be the amount carried from column j to column $j+1$ when n m-digit base-b numbers are added, and the digits of these numbers are chosen uniformly and independently in $\{0, 1, \ldots, b-1\}$.

Theorem 4.1. *For $1 \le j \le m$ and $n \ge 2$, the expected value of κ_j is*

$$\mu_j = \frac{n-1}{2}\left(1 - \frac{1}{b^j}\right).$$

The variance of κ_j is

$$\sigma_j^2 = \frac{n+1}{12}\left(1 - \frac{1}{b^{2j}}\right).$$

Normalized by its mean and variance, for large n, κ_j has a limiting standard normal distribution.

Proof. From Lemma 3.3, κ_j is distributed exactly like the number of descents among the n rows of the rightmost j digits of the random array. The distribution of these descents is studied in [**8**] where they are shown to be a 1-dependent process with the required mean and variance. The central limit theorem for 1-dependent processes is classical [**3**]. ∎

Remarks.

1. Observe that μ_j and σ_j^2 are increasing to their respective limiting values $(n-1)/2$, $(n+1)/12$ as j increases.

   A Markov chain P on the integers is called stochastically monotone if for any up-set U (that is, a set of the form $U = \{l : l \geq k\}$), one has that $P(i, U) \geq P(h, U)$ whenever $i \geq h$. Here $P(i, U) = \sum_{j \in U} P(i, j)$ denotes the probability that the chain is in a state in U at some step given that it was in state i at the previous step. The carries chain is clearly stochastically monotone (starting with a carry of i rather than a carry of $h \leq i$ can only increase the carry at the next step). This monotonicity was used in our analysis of the total variation distance convergence rate of the carries chain in the companion paper [**15**], and a referee notes that it gives another proof that $\mu_{j+1} \geq \mu_j$. Namely, since P is stochastically monotone, so is each power P^j. Thus the distributions $P^j(0, \cdot)$ increase stochastically in j (meaning that $P^{j+1}(0, U) \geq P^j(0, U)$ for any up-set U). Indeed,

$$P^{j+1}(0, U) = \sum_i P(0, i) P^j(i, U) \geq \sum_i P(0, i) P^j(0, U) = P^j(0, U).$$

   This precisely says that the successive carry random variables κ_j increase stochastically, so their expected values are nondecreasing too.

2. Let $S_m = \kappa_1 + \kappa_2 + \cdots + \kappa_m$ be the total number of carries. By linearity of expectation and Theorem 4.1, this has mean

$$\bar{\mu}_m = \frac{n-1}{2}\left(m - \frac{1}{b-1}\left(1 - \frac{1}{b^m}\right)\right).$$

   When $n = 2$, this was shown by Knuth [**25**, p. 278]. He also finds the variance of S_m when $n = 2$. For fixed n and b, the central limit theorem for finite state space Markov chains [**7**] shows that S_m, normalized by its mean and variance, has a standard normal limiting distribution.

3. The fine properties of the number of carries within a column are studied in [**8**] where it is shown to be a determinantal point process.

As shown above, the carries process κ_j, $0 \leq j \leq m$ (with $\kappa_0 = 0$) is a Markov chain which has limiting stationary distribution $\pi(j) = A(n, j)/n!$. To study the rate of convergence to the limit we first prove a new property of the amazing matrix $(P(i, j))$ of **(H1)**. Recall that a matrix is totally positive of order two (TP_2) if all the 2×2 minors are nonnegative (matrices in which all minors are positive are called strictly totally positive). The argument for Lemma 4.2 was suggested by Alexei Borodin.

Lemma 4.2. *For every n and b, the matrix $(P(i, j))$ of* **(H1)** *is TP_2.*

Proof. As noted on [**22**, p. 140],

$$P(i, j) = \frac{1}{b^n}\left[x^{(j+1)b-i-1}\right]\left(\frac{1-x^b}{1-x}\right)^{n+1}$$

where $[x^k]f(x)$ is the coefficient of x^k in a polynomial $f(x)$. Consider the infinite matrix M_n with (i, j)-coordinate $1/b^n \cdot [x^{i-j}]\left((1-x^b)/(1-x)\right)^{n+1}$. As the transpose

of P is a submatrix of M_n, it will suffice to show that M_n is TP_2. Since the product of TP_2 matrices is TP_2 and $M_n = 1/b^n \cdot (M_0)^{n+1}$, it is enough to treat the case $n = 0$. Now, M_0 is lower triangular with ones down the diagonal, ones on the next lowest $b-1$ diagonals and zeros elsewhere. For example, when $b = 3$ the relevant matrix is

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & \cdots \\ 1 & 1 & 0 & 0 & 0 & 0 & \cdots \\ 1 & 1 & 1 & 0 & 0 & 0 & \cdots \\ 0 & 1 & 1 & 1 & 0 & 0 & \cdots \\ 0 & 0 & 1 & 1 & 1 & 0 & \cdots \\ & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots \end{pmatrix}.$$

Since (for general b) the 1's occur in consecutive diagonal bands, the matrices

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix},$$

cannot occur as submatrices. As these are the only 2×2 zero-one matrices with negative determinant, the lemma follows. ∎

Remark. When $b = 2$, the original $(P(i, j)) = \left(2^{-n}\binom{n+1}{2j-i+1}\right)$ is totally positive (TP_∞). Indeed, $P(i, j) = 2^{-n}[x^{2j-i+1}](1+x)^{n+1}$. Letting $i' = i+1$ and $j' = j+1$, this becomes $2^{-n}[x^{2j'-i'}](1+x)^{n+1}$. Thus each minor of $(P(i, j))$ is a subminor of the matrix with entries $2^{-n}[x^{j'-i'}](1+x)^{n+1}$. This is totally positive by the classification of Polya frequency sequences due to Schoenberg and Edrei [**24**, Chapter 8]. We have yet to settle whether $(P(i, j))$ is TP_∞ for general b, but note by **(H4)** that since the product of TP_∞ matrices is TP_∞, total positivity does hold when b is a power of 2.

Consider the basic transition matrix $(P(i, j))$ for general b and n. This has stationary distribution $\pi(j)$, $0 \le j \le n-1$, given in **(H2)**. The carries Markov chain starts at 0 and the rightmost carries tend to be smaller. This is seen in Theorem 4.1 and Remark 1 following it. It is natural to ask how far over one must go so that the carries process is stationary. If $P^r(0, j)$ is the chance of a carry of j after r steps, we measure the approach to stationarity by the separation

$$\text{sep}(r) = \max_j \left[1 - \frac{P^r(0, j)}{\pi(j)}\right].$$

Thus $0 \le \text{sep}(r) \le 1$ and $\text{sep}(r)$ is small provided $P^r(0, j)$ is close to $\pi(j)$ for all j. See [**2**] or [**14**] for further properties of separation. The following theorem may be roughly summarized as showing that convergence requires $r = 2\log_b n$.

Theorem 4.3. *For any $b \ge 2$ and $n \ge 2$, the transition matrix $(P(i, j))$ of* **(H1)** *satisfies:*

1. *For all $r \ge 0$, the separation $sep(r)$ of the carries chain after r steps (started at 0) is attained at the state $j = n-1$.*
2. *For $r = \lfloor 2\log_b(n) + \log_b(c) \rfloor$,*

$$sep(r) \to 1 - e^{-1/2c}$$

if $c > 0$ is fixed and $n \to \infty$.

Proof. By Lemma 4.2, the matrix $(P(i, j))$ is TP_2. Thus the matrix P^* with (i, j)-entry $P^*(i, j) := [P(j, i)\pi(j)]/\pi(i)$ is also TP_2, since every 2×2 minor of P^* is a positive multiple of a 2×2 minor of P. Now consider the vector whose ith component is $f_r(i) = P^r(0, i)/\pi(i)$. We claim that $P^* f_r = f_{r+1}$. Indeed,

$$\begin{aligned}
[P^* f_r](i) &= \sum_j P^*(i, j) f_r(j) \\
&= \sum_j P^*(i, j) \frac{P^r(0, j)}{\pi(j)} \\
&= \sum_j \frac{P(j, i)\pi(j)}{\pi(i)} \frac{P^r(0, j)}{\pi(j)} \\
&= \frac{P^{r+1}(0, i)}{\pi(i)} \\
&= f_{r+1}(i).
\end{aligned}$$

Now the "variation-diminishing property" [**24**, p. 22] implies that if f is monotone and P^* is TP_2, then $P^* f$ is monotone. Since f_0 is monotone (the walk is started at 0), it follows that f_r is monotone, i.e., that the separation $\mathrm{sep}(r)$ is attained at the state $n - 1$.

For the second assertion, note that by the relation between riffle shuffling and the carries chain in Theorem 3.1, $P^r(0, n - 1)$ is equal to the chance of being at the unique permutation with $n - 1$ descents after r iterations of a b-shuffle; by equation (4) in Section 2 this is $b^{-rn}\binom{b^r}{n}$. Thus

$$\begin{aligned}
\mathrm{sep}(r) &= 1 - \frac{P^r(0, n - 1)}{\pi(n - 1)} \\
&= 1 - \prod_{i=0}^{n-1} \left(1 - \frac{i}{b^r}\right) \\
&= 1 - \exp\left(\sum_{i=0}^{n-1} \log\left(1 - \frac{i}{b^r}\right)\right).
\end{aligned}$$

Letting $b^r = cn^2$ with $c > 0$ fixed, this becomes

$$1 - \exp\left(-\sum_{i=0}^{n-1}\left[\frac{i}{cn^2} + O\left(\frac{i^2}{n^4}\right)\right]\right) \to 1 - e^{-1/2c},$$

as $n \to \infty$. ∎

Remark. It is known [**5**] that it takes $r = 2\log_b n$ b-shuffles to make separation small on the symmetric group. Via Theorem 3.1, this shows $2\log_b n$ steps suffice for the carries process. Of course, a priori fewer steps might suffice but Theorem 4.3 shows the result is sharp for large n. In mild contrast, it is known [**1, 5**] that $(3/2)\log_2 n$ "ordinary" ($b = 2$) riffle shuffles are necessary and suffice for total variation convergence. Our companion paper [**15**] shows that $(1/2)\log_b n$ carry steps are necessary and suffice for total variation convergence.

5. THREE RELATED TOPICS. The "amazing matrix" turns up in different contexts (sections of generating functions) in the work of Brenti and Welker [**9**]. There is an analog of carries for multiplication which has interesting structure. Finally, there are quite different amazing matrices having many of the same properties as Holte's. These three topics are briefly developed in this section.

5.1. Sections of generating functions. Some natural sequences a_k, $0 \le k < \infty$ have generating functions

$$\sum_{k=0}^{\infty} a_k x^k = \frac{h(x)}{(1-x)^{n+1}} \tag{5}$$

with $h(x) = h_0 + h_1 x + \cdots + h_{n+1} x^{n+1}$ a polynomial of degree at most $n+1$. For example, the generating function of $a_k = k^n$ has this form with $h(x) = \sum_{j \ge 0} A(n, j) x^{j+1}$ with $A(n, j)$ the Eulerian numbers of **(H2)**. Rational generating functions characterize sequences $\{a_h\}$ which satisfy a constant coefficient recurrence [**28**]. They arise naturally as the Hilbert series of graded algebras [**17**, Chapter 10.4].

Suppose we are interested in every bth term $\{a_{bk}\}$, $0 \le k < \infty$. It is not hard to see that

$$\sum_{k=0}^{\infty} a_{bk} x^k = \frac{h^{(b)}(x)}{(1-x)^{n+1}}$$

for another polynomial $h^{(b)}(x)$ of degree at most $n+1$. Brenti and Welker [**9**] show that the ith coefficient of $h^{(b)}(x)$ satisfies

$$h_i^{(b)} = \sum_{j=0}^{n+1} C(i, j) h_j$$

with C an $(n+2) \times (n+2)$ matrix with (i, j)-entry $(0 \le i, j \le n+1)$ equal to the number of solutions to $a_1 + \cdots + a_{n+1} = ib - j$ where $0 \le a_l \le b-1$ are integers. The carries matrix is closely related to their matrix. Indeed, remove from C the $i = 0, n+1$ rows and the $j = 0, n+1$ columns. Let $i' = i - 1$, $j' = j - 1$. This gives an $n \times n$ matrix with (i', j')-entry $(0 \le i', j' \le n-1)$ equal to the number of solutions to $a_1 + \cdots + a_{n+1} = (i'+1)b - (j'+1)$ where $0 \le a_l \le b-1$ are integers. Multiplying by b^{-n} and taking transposes gives the carries matrix for mod b addition of n numbers (see the formula for the carries matrix on [**22**, p. 140]). Brenti and Welker [**9**] and Beck and Stapledon [**6**] develop some properties of the transformation C. We hope some of the facts from the present development (in particular the central limit theorems satisfied by the coefficients and results on convergence rates) will illuminate their algebraic applications; see [**15**] for a result in this direction.

5.2. Carries for multiplication. Consider the process of base-b multiplication of a random number (digits chosen from the uniform distribution on $\{0, 1, \ldots, b-1\}$) by a fixed number $k > 0$. We do not require that k is single-digit. Then there is a natural way to define a carries process, which is best defined by example. Let $k = 26$ and consider multiplying 1423 by 26 base 10. The zeroth carry is defined as $\kappa_0 = 0$. To compute the first carry, note that $26 \times 3 = 78$, so $\kappa_1 = 7$. Then $\kappa_1 + 26 \times 2 = 59$, so $\kappa_2 = 5$. Next $\kappa_2 + 26 \times 4 = 109$, so $\kappa_3 = 10$. Finally, $\kappa_3 + 26 \times 1 = 36$, so $\kappa_4 = 3$. The carries in this multiplication process are equal to those arising from adding k copies of the same random number (so 26 copies of 1423 in the example).

It is not difficult to see that the above process is a Markov chain on the state space $\{0, 1, \ldots, k-1\}$. For example, if $b = 10$ and $k = 7$, the transition matrix is

$$K(i,j) = \frac{1}{10}\begin{bmatrix} 2 & 1 & 2 & 1 & 2 & 1 & 1 \\ 2 & 1 & 2 & 1 & 1 & 2 & 1 \\ 2 & 1 & 1 & 2 & 1 & 2 & 1 \\ 1 & 2 & 1 & 2 & 1 & 2 & 1 \\ 1 & 2 & 1 & 2 & 1 & 1 & 2 \\ 1 & 2 & 1 & 1 & 2 & 1 & 2 \\ 1 & 1 & 2 & 1 & 2 & 1 & 2 \end{bmatrix}$$

The matrix K above does not have all eigenvalues real, but the following properties do hold in general:

- K is doubly stochastic, meaning that every row and column sums to 1.
- K is a generalized circulant matrix, meaning that each column is obtained from the previous column by shifting it downward by b mod k.
- Fix k and let K_a and K_b be the base-a and base-b transition matrices for multiplication by k. Then $K_{ab} = K_a K_b$.

The first two properties are at the level of undergraduate exercises, and [**13**, Chapter 5] is a useful reference for generalized circulants. The third property holds for the same reason that it does for Holte's matrix (see the explanation on [**22**, p. 143]).

Since K is doubly stochastic, the carries chain for multiplication has the uniform distribution on $\{0, 1, \ldots, k-1\}$ as its stationary distribution. Concerning convergence rates, one has the following simple upper bound for total variation distance.

Proposition 5.1. *Let K_0^r denote the distribution of the carries chain for multiplication by k base-b after r steps, started at the state 0. Let π denote the uniform distribution on $\{0, 1, \ldots, k-1\}$. Then*

$$\frac{1}{2}\sum_{j=0}^{k-1} |K_0^r(j) - \pi(j)| \le \frac{k}{2b^r}.$$

Proof. Observe that

$$K_0^r(j) = \frac{1}{b^r}\left|\{x : jb^r \le kx < (j+1)b^r, 0 \le x < b^r\}\right|.$$

The number of integers x satisfying $jb^r/k \le x < (j+1)b^r/k$ is between $(b^r/k) - 1$ and $(b^r/k) + 1$. Hence $|K_0^r(j) - \pi(j)| \le 1/b^r$, and the result follows by summing over j. ∎

Convergence rate lower bounds depend on the number-theoretic relation of k and b in a complicated way. For instance if $k = b$, the process is exactly random after 1 step.

5.3. Another amazing matrix. From one point of view, Holte's amazing matrix exists because there is a "big" Markov chain on the symmetric group S_n with eigenvalues $1, 1/b, 1/b^2, \ldots, 1/b^{n-1}$ and a function $T : S_n \to \{0, 1, \ldots, n-1\}$ such that the image of this Markov chain is Holte's Markov chain of carries. (The chain on S_n is the

b-shuffle Markov chain, and the function T assigns to each permutation the number of descents). Of course, the interpretation as "carries" remains amazing.

There are many functions of the basic riffle shuffling Markov chain which remain Markov chains. Here is a simple one. Consider repeated shuffling of a deck of n cards using the b-shuffles described in Section 2. The position of the card labeled "one" gives a Markov chain on $\{1, 2, \ldots, n\}$. In [**4**] the transition matrix of this chain is shown to be

$$Q_b(i, j) = \frac{1}{b^n} \times \tag{6}$$

$$\sum_{h=1}^{b} \sum_{r=\ell}^{u} \binom{j-1}{r} \binom{n-j}{i-r-1} h^r (b-h)^{j-1-r} (h-1)^{i-1-r} (b-h+1)^{(n-j)-(i-r-1)}$$

where the inner sum is from $\ell = \max(0, (i + j) - (n + 1))$ to $u = \min(i - 1, j - 1)$. For example, when $n = 2$ and 3 the matrices are

$$\frac{1}{2b} \begin{pmatrix} b+1 & b-1 \\ b-1 & b+1 \end{pmatrix},$$

$$\frac{1}{6b^2} \begin{pmatrix} (b+1)(2b+1) & 2(b^2-1) & (b-1)(2b-1) \\ 2(b^2-1) & 2(b^2+2) & 2(b^2-1) \\ (b-1)(2b-1) & 2(b^2-1) & (b+1)(2b+1) \end{pmatrix}.$$

Ciucu [**11**] (see also [**4**]) proves that Q_b satisfies:

- Q_b has eigenvalues $1, 1/b, 1/b^2, \ldots, 1/b^{n-1}$.
- The eigenvectors of Q_b do not depend on b; in particular, the stationary distribution is uniform: $\pi(i) = 1/n$, $1 \le i \le n$.
- $Q_a Q_b = Q_{ab}$.

We suspect that Q_b has other nice properties and appearances.

ACKNOWLEDGMENTS. We thank Alexei Borodin for help with total positivity, Francesco Brenti for telling us about sections of generating functions, Jim Fill for giving us his discovery of the crucial bar map, and Phil Hanlon for daring to suggest that the two Markov chains were the same. We thank two careful referees for their comments. The work of Diaconis was supported by NSF grant DMS-0505673 and the chair d'excellence at the University of Nice, Sophia-Antipolis. The work of Fulman was supported by NSF grant DMS-0503901.

REFERENCES

1. D. Aldous, Random walks on finite groups and rapidly mixing Markov chains, in *Séminaire de Probabilités XVII,* Lecture Notes in Mathematics, vol. 986, Springer, New York, 1983, 243–297. doi: 10.1007/BFb0068322
2. D. Aldous and P. Diaconis, Shuffling cards and stopping times, this MONTHLY **93** (1986) 333–348. doi: 10.2307/2323590
3. T. W. Anderson, *The Statistical Analysis of Time Series*, John Wiley, New York, 1971.
4. S. Asaf, P. Diaconis, and K. Soundararajan, A rule of thumb for riffle shuffling (preprint), Department of Statistics, Stanford University, Stanford, CA, 2008.
5. D. Bayer and P. Diaconis, Trailing the dovetail shuffle to its lair, *Ann. Appl. Probab.* **2** (1992) 294–313. doi:10.1214/aoap/1177005705
6. M. Beck and A. Stapledon, On the log-concavity of Hilbert series of Veronese subrings and Ehrhart series (2008), available at http://xxx.lanl.gov/abs/0804.3639.
7. P. Billingsley, *Probability and Measure*, John Wiley, New York, 1986.

8. A. Borodin, P. Diaconis, and J. Fulman, On adding a list of numbers (and other one-dependent determinantal processes) (2009), available at http://xxx.lanl.gov/abs/0904.3740.
9. F. Brenti and V. Welker, The Veronese construction for formal power series and graded algebras, *Adv. in Appl. Math.* **42** (2009) 545–556. doi:10.1016/j.aam.2009.01.001
10. J. Buhler, D. Eisenbud, R. Graham, and C. Wright, Juggling drops and descents, this MONTHLY **101** (1994) 507–519. doi:10.2307/2975316
11. M. Ciucu, No-feedback card guessing for dovetail shuffles, *Ann. Appl. Probab.* **8** (1998) 1251–1269. doi:10.1214/aoap/1028903379
12. L. Comtet, *Advanced Combinatorics*, D. Reidel, Dordrecht, 1974.
13. P. Davis, *Circulant Matrices*, John Wiley, New York, 1979.
14. P. Diaconis, Mathematical developments from the analysis of riffle-shuffling, in *Groups, Combinatorics and Geometry*, A. Ivanov, M. Liebeck, and J. Saxl, eds., World Scientific, River Edge, NJ, 2003, 73–97.
15. P. Diaconis and J. Fulman, Carries, shuffling, and symmetric functions, *Adv. in Appl. Math.* **43** (2009) 176–196. doi:10.1016/j.aam.2009.02.002
16. P. Diaconis, M. McGrath, and J. Pitman, Riffle shuffles, cycles and descents, *Combinatorica* **15** (1995) 11–29. doi:10.1007/BF01294457
17. D. Eisenbud, *Commutative Algebra with a View Toward Algebraic Geometry*, Springer-Verlag, New York, 2004.
18. J. Fulman, Applications of the Brauer complex: card shuffling, permutation statistics, and dynamical systems, *J. Algebra* **243** (2001) 96–122. doi:10.1006/jabr.2001.8814
19. ———, Applications of symmetric functions to cycle and increasing subsequence structure after shuffles, *J. Algebraic Comb.* **16** (2002) 165–194. doi:10.1023/A:1021177012548
20. E. Gilbert, Theory of shuffling, Technical Report MM-55-114-44, Bell Telephone Laboratories, Murray Hill, NJ, 1955.
21. P. Hanlon, The action of S_n on the components of the decomposition of Hochschild homology, *Michigan Math. J.* **37** (1990) 105–124. doi:10.1307/mmj/1029004069
22. J. Holte, Carries, combinatorics, and an amazing matrix, this MONTHLY **104** (1997) 138–149. doi:10.2307/2974981
23. D. Isaksen, A cohomological viewpoint on elementary school arithmetic, this MONTHLY **109** (2002) 796–805. doi:10.2307/3072368
24. S. Karlin, *Total Positivity*, vol. 1, Stanford University Press, Stanford, CA, 1968.
25. D. E. Knuth, *The Art of Computer Programming*, vol. 2, 3rd ed., Addison-Wesley, Reading, MA, 1997.
26. ———, *The Art of Computer Programming*, vol. 3, 2nd ed., Addison-Wesley, Reading, MA, 1998.
27. B. Mann, How many times should you shuffle a deck of cards? *UMAP J.* **15** (1994) 303–332; reprinted in J. L. Snell, ed., *Topics in Contemporary Probability and Its Applications*, Probability and Stochastics Series, CRC Press, Boca Raton, FL, 1995, 261–289.
28. R. P. Stanley, *Enumerative Combinatorics I*, 2nd ed., Cambridge University Press, Cambridge, 1997.

PERSI DIACONIS shuffled his first deck of cards at the age of 5, and read his first probability book at the age of 15. As a professional magician and mathematician, he has been shuffling and computing probabilities ever since. He currently teaches at Stanford University.
Department of Mathematics and Statistics, Stanford University, Stanford, CA 94305

JASON FULMAN received his Ph.D. from Harvard University in 1997. He enjoys the communication and discovery of new mathematics, and currently teaches at the University of Southern California.
Department of Mathematics, University of Southern California, Los Angeles, CA 90089-2532
fulman@usc.edu