# NO-FEEDBACK CARD GUESSING FOR DOVETAIL SHUFFLES


Mihai Ciucu

Institute for Advanced Study
School of Mathematics
Princeton, New Jersey 08540


December, 1997


Abstract. We consider the following problem. A deck of $2n$ cards labeled consecutively from 1 on top to $2n$ on bottom is face down on the table. The deck is given $k$ dovetail shuffles and placed back on the table, face down. A guesser tries to guess at the cards one at a time, starting from top. The identity of the card guessed at is not revealed, nor is the guesser told whether a particular guess was correct or not. The goal is to maximize the number of correct guesses. We show that for $k \geq 2\log_2(2n)+1$ the best strategy is to guess card 1 for the first half of the deck and card $2n$ for the second half. This result can be interpreted as indicating that it suffices to perform the order of $\log_2(2n)$ shuffles to obtain a well mixed deck, a fact proved by Bayer and Diaconis [3]. We also show that if $k = c\log_2(2n)$ with $1 < c < 2$ then the above guessing strategy is not the best.


## 1. Introduction

Consider a deck of $n$ cards and label the possible cutting places of the deck by $0, 1, \ldots, n$, starting from top. A *dovetail shuffle* (or *riffle shuffle*) consists of (1) cutting the deck at a position selected at random according to the binomial distribution and (2) interleaving the two resulting decks at random, according to the uniform distribution on all possible interleavings.

This mathematical model for shuffling was introduced by E. Gilbert and C. Shannon in unpublished work at Bell Labs in 1956. It was further developed by J. Reeds in unpublished work in 1976. The first published study is Aldous [**1**] who sketched an argument that $(3/2)\log_2 n$ shuffles suffice to mix up $n$ cards. Aldous and Diaconis [**2**] gave a careful proof that $2\log_2 n$ shuffles are necessary and suffice for separation distance. Diaconis [**4**] gives a practical analysis showing that the Gilbert-Shannon-Reeds model is a good model for the way real people shuffle cards. The definitive work on shuffling was done by Bayer and Diaconis [**3**] followed by Diaconis, McGrath and Pitman [**5**]. The first paper gives a clear proof that $(3/2)\log_2 n + c$ shuffles are necessary and suffice by giving a closed form formula for the chance that the deck is in any given arrangement after any number of shuffles (an excellent expository account of this work is given by Mann [**7**]). The second paper determines the cycle structure, showing that such features as the number of fixed points get random after any growing number of shuffles. A recent extension of the Gilbert-Shannon-Reeds model is given by Lalley [**6**].

We consider the following problem. A deck of $2n$ cards labeled consecutively from 1 on top to $2n$ on bottom is face down on the table. The deck is given $k$ riffle shuffles and placed back on the table, face down. A guesser tries to guess at the cards one at a time, starting from top. During this process the guesser is given no feedback, i.e., the identity of the card guessed at is not revealed, nor is he told whether a particular guess was correct or not. The question is to find a guessing strategy which maximizes the expected number of correct guesses. In case there exists a unique such strategy, we call it the best strategy.

The main result of this paper is the following.

THEOREM 1.1.

*(a) For $k \geq 2\log_2(2n)+1$, the best guessing strategy after $k$ riffle shufflings of a deck of $2n$ cards is to guess 1 at the first $n$ cards and $2n$ at the remaining $n$.*

*(b) Suppose $1 < c < 2$ and $n \geq n(c)$, where $n(c)$ is some positive integer depending on $c$. Then if the deck has been given $c\log_2(2n)$ riffle shuffles, the above guessing strategy does not maximize the expected number of correct guesses.*

In Section 5 we indicate a way of using our guessing problem to measure how well a deck of cards is mixed. We argue that for even $n$ a number of the order of $\log_2(n)$ shuffles suffices to mix well a deck of $n$ cards. This is in accordance with a result of Bayer and Diaconis [**3**] stating that the total variation distance from the probability distribution obtained after $k$ riffle shuffles to the uniform distribution drops abruptly around $k = (3/2)\log_2 n$ from being very close to 1 to being very close to zero. However, unlike in the case of total variation distance, for our measure of well-mixedness there is no cutoff phenomenon (this is not surprising, since numerical evidence presented in [**3**] suggests this is the case for a similarly defined measure in the situation of complete feedback).

## 2. The position matrix

Suppose we have a deck of $n$ cards, labeled consecutively starting with 1 on top and ending with $n$ on the bottom. The *position matrix* $M = M_n$ is the $n \times n$ matrix whose $(i, j)$ entry is the probability that the card labeled $i$ ends up in position $j$ after a riffle shuffle (card position $i$ is the slot between cut positions $i-1$ and $i$, $i = 1, \ldots, n$).

LEMMA 2.1. *For $1 \leq i, j \leq n$ we have*

$$M_{ii} = \frac{1}{2^n}(2^{i-1} + 2^{n-i}) \tag{2.1}$$

$$M_{ij} = \frac{1}{2^{n-j+1}}\binom{n-j}{i-j}, \quad \text{for } i > j \tag{2.2}$$

$$M_{ij} = M_{n-i+1,n-j+1}. \tag{2.3}$$

*Proof.* Imagine having a second set of numbers on our cards, one in which the cards are labeled consecutively from 1 on *bottom* through $n$ on top. Call this the "upward labeling"; call the original labeling the "downward labeling."

It is clear that, after a riffle shuffle, card $i$ ends up in position $j$ in downward labeling if and only if card $n-i+1$ goes to position $n-j+1$ in upward labeling. Since the probability distributions involved in the riffle shuffle have a vertical symmetry axis, we obtain (2.3).

Since we are cutting by the binomial distribution and we have $\binom{n}{k}$ equally likely interleavings after a cut at position $k$, each sequence "cut followed by interleaving" occurs with probability $1/2^n$. Therefore, to determine $M_{ij}$ it suffices to count the number of cut-interleavings in which card $i$ ends up in position $j$.

Let $i > j$. If the cut was made at position $k \geq i$, then the $i-1$ cards preceding card $i$ in the upper deck will still precede it after the interleaving, thus preventing card $i$ from occupying position $j$.

Suppose therefore that the cut was made at some position $k < i$. The cards labeled $k+1$, $k+2, \ldots, i-1$ ($i-k-1$ in number) will always precede card $i$ after the shuffle. In order that card $i$ ends up in position $j$, we need $j-i+k$ cards from the upper deck to be interleaved above it. Since these have to be the first $j-i+k$ cards of the upper deck, one can do this in $\binom{j-1}{j-i+k}$ ways. To complete the shuffle, we have to interleave the remaining $i-j$ cards in the top deck below card $i$; this can be achieved in $\binom{n-j}{i-j}$ ways.

Therefore, the total number of interleavings sending card $i$ to position $j$ is

$$\sum_k \binom{j-1}{j-i+k}\binom{n-j}{i-j} = 2^{j-1}\binom{n-j}{i-j},$$

thus proving (2.2).

Finally, consider the case $i = j$. The above discussion yields $2^{i-1}\binom{n-i}{0} = 2^{i-1}$ interleavings sending card $i$ to position $i$. However, we obtain some more by cutting at positions $k \geq i$: there are $\binom{n-i}{k-i}$ interleavings of the resulting decks for which card $i$ occupies position $i$. Summing over $k$, this gives an additional term of $2^{n-i}$, thus proving (2.1). $\square$

The crucial fact in our proof of Theorem 1.1 is that we can determine explicitly the eigenvalues and eigenvectors of the position matrix $M$.

For $m \geq 0$, let $u_m \in \mathbf{R}^n$ be the column vector with $i$-th component $(-1)^{i-1}\binom{m}{i-1}$, $i = 1, \ldots, n$. Let $u'_m$ be the column vector obtained from $(-1)^{m-1}u_m$ by reading its components from bottom to top (i.e., the $i$-th component of $u'_m$ is $(-1)^{n-i+m-1}\binom{m}{n-i}$). Denote by $v_0 \in \mathbf{R}^n$ the column vector with all coordinates equal to 1, and define $v_m := u_{m-1} + u'_{m-1}$, for $m = 1, 2, \ldots, n-1$. In other words, for $1 \leq m \leq n-1$ and $1 \leq i \leq n$ we set

$$v_m(i) := (-1)^{i-1}\binom{m-1}{i-1} + (-1)^{n-i+m}\binom{m-1}{n-i}, \tag{2.4}$$

where $v(i)$ denotes the $i$-th component of the vector $v$.

THEOREM 2.2. *For $0 \leq m \leq n-1$, $v_m$ is an eigenvector of the position matrix $M$, with corresponding eigenvalue $1/2^m$.*

One may wonder how could one guess the eigenvalues, and especially the eigenvectors, of $M = M_n$. This can be done for example by computing them explicitly for small values of $n$, using a linear algebra package on the computer. The pattern of the eigenvalues is then easily recognized. Normalizing the eigenvectors so that their first coordinates are 1, the coordinates of the eigenvector corresponding to the eigenvalue $1/2^{n-1}$ are readily identified as signed binomial coefficients. After some experimentation one arrives at conjecturing that the eigenvectors are given by (2.4).

*Proof.* As a consequence of the definition, all row sums of $M$ equal 1. Therefore, $v_0$ is an eigenvector with eigenvalue 1.

Let $r_k$ denote the $k$-th row of $M$. To prove the Theorem, we have to show that for all $1 \le k \le n$ (and all $0 \le m \le n-2$) we have

$$2^n r_k \cdot u_m + 2^n r_k \cdot u_m' = 2^{n-m-1}\left((-1)^{k-1}\binom{m}{k-1} + (-1)^{n-k+m-1}\binom{m}{n-k}\right), \tag{2.5}$$

where the dot on the left hand side denotes the usual scalar product of vectors. Using Lemma 2.1, the first term on the left hand side of (2.5) can be written as

$$\begin{aligned} 2^n r_k \cdot u_m &= \sum_{i=0}^{k-2}(-2)^i\binom{m}{i}\binom{n-i-1}{k-i-1} \\ &\quad + (-1)^{k-1}\binom{m}{k-1}\left(2^{k-1}\binom{n-k}{0} + 2^{n-k}\binom{k-1}{0}\right) \\ &\quad + (-1)^m 2^{n-m-1}\sum_{i=0}^{m-k}(-2)^i\binom{m}{i}\binom{m-i}{k-1} \\ &= \sum_{i=0}^{k-1}(-2)^i\binom{m}{i}\binom{n-i-1}{k-i-1} \\ &\quad + (-1)^m 2^{n-m-1}\sum_{i=0}^{m-k+1}(-2)^i\binom{m}{i}\binom{m-i}{k-1}. \end{aligned} \tag{2.6}$$

Similarly, one obtains that

$$\begin{aligned} 2^n r_k \cdot u_m' &= (-1)^{m-1}\sum_{i=0}^{n-k}(-2)^i\binom{m}{i}\binom{n-i-1}{n-i-k} \\ &\quad - 2^{n-m-1}\sum_{i=0}^{m-n+k}(-2)^i\binom{m}{i}\binom{m-i}{n-k}. \end{aligned} \tag{2.7}$$

To prove (2.5) we proceed as follows: first, we show that the last sum in (2.6) is equal to the first term in (the expansion of) the right hand side of (2.5); second, we show that the second sum on the right hand side of (2.7) equals the second term on the right hand side of (2.5); and third, we show that the second to last sum in (2.6) is the negative of the first sum on the right in (2.7).

After some manipulation, the three claims above are seen to be equivalent to the following three equalities:

$$\sum_{i=0}^{m-k+1} (-2)^i \binom{m}{i} \binom{m-i}{k-1} = (-1)^{m-k+1} \binom{m}{m-k+1} \tag{2.8}$$

$$\sum_{i=0}^{m-n+k} (-2)^i \binom{m}{i} \binom{m-i}{n-k} = (-1)^{m-n+k} \binom{m}{m-n+k} \tag{2.9}$$

$$\sum_{i=0}^{k-1} (-2)^i \binom{m}{i} \binom{n-i-1}{k-i-1} = (-1)^m \sum_{i=0}^{n-k} (-2)^i \binom{m}{i} \binom{n-i-1}{n-i-k}. \tag{2.10}$$

The first two equalities are clearly equivalent: one is obtained from the other by replacing $k$ by $n-k+1$. Replacing $k$ by $k+1$ in (2.8), the identity to be proved becomes

$$\sum_{i=0}^{m-k} (-2)^i \binom{m}{i} \binom{m-i}{k} = (-1)^{m-k} \binom{m}{m-k}.$$

However, one has more generally that

$$\sum_{i \geq 0} x^i \binom{m}{i} \binom{m-i}{k} = (x+1)^{m-k} \binom{m}{m-k},$$

since the coefficients of $x^i$ on the left and right hand sides of the above relation are readily seen to be equal.

To complete the proof, we need to verify identity (2.10). This will follow from Lemma 2.4 by replacing $n$ by $n-1$ and $k$ by $k-1$. □

The following identity is proved in [**8**, p.8].

LEMMA 2.3. $\sum_{i \geq 0} (-1)^i \binom{n-i}{m-i} \binom{p}{i} = \binom{n-p}{m}$.

For nonnegative integers $m, n$ and $k$, define

$$f(m,n,k) := \sum_{i=0}^{k} (-2)^i \binom{m}{i} \binom{n-i}{k-i}.$$

LEMMA 2.4. $f(m,n,k) = (-1)^m f(m,n,n-k)$.

*Proof.* We have

$$
\begin{aligned}
f(m,n,k) &= \sum_{i=0}^{k}(-2)^i\binom{m}{i}\binom{n-i}{n-k} \\
&= \sum_{i=0}^{k}(-1)^i\binom{m}{i}\binom{n-i}{n-k}\sum_{j=0}^{i}\binom{i}{j} \\
&= \sum_{j=0}^{k}\sum_{i=j}^{k}(-1)^i\binom{m}{i}\binom{i}{j}\binom{n-i}{n-k} \\
&= \sum_{j=0}^{k}\binom{m}{j}\sum_{i=j}^{k}(-1)^i\binom{m-j}{i-j}\binom{n-i}{n-k} \\
&= \sum_{j=0}^{k}\binom{m}{j}\sum_{i\ge 0}(-1)^{i+j}\binom{m-j}{i}\binom{n-j-i}{n-k},
\end{aligned}
\tag{2.11}
$$

where at the fourth equality we used that $\binom{m}{i}\binom{i}{j} = \binom{m}{j}\binom{m-j}{i-j}$.

Replacing simultaneously $p \leftarrow m-j$, $n \leftarrow n-j$ and $m \leftarrow k-j$ in Lemma 2.3, we obtain

$$
\sum_{i\ge 0}(-1)^i\binom{m-j}{i}\binom{n-j-i}{k-j-i} = \binom{n-m}{k-j}.
$$

Therefore, we can continue the sequence of equalities (2.11) and obtain

$$
f(m,n,k) = \sum_{j=0}^{k}(-1)^j\binom{m}{j}\binom{n-m}{k-j}.
$$

Thus, if $Q = Q_{m,n}$ is the polynomial $(1-x)^m(1+x)^{n-m}$, then $f(m,n,k)$ is just the coefficient of $x^k$ in $Q$. Let $Q = \sum_{\nu\ge 0} a_\nu x^\nu$. The statement of the Lemma is then equivalent to

$$
a_k = (-1)^m a_{n-k}.
$$

However, this follows because

$$
\begin{aligned}
x^n Q(x^{-1}) &= x^n(1-x^{-1})^m(1+x^{-1})^{n-m} \\
&= (x-1)^m(x+1)^{n-m} \\
&= (-1)^m(1-x)^m(1+x)^{n-m} \\
&= (-1)^m Q(x). \ \square
\end{aligned}
$$

Denote by $P = P_n$ the matrix whose $i$-th column is $v_{i-1}$, for $i = 1,\dots,n$. It follows from Theorem 2.2 that $P^{-1}MP$ is the diagonal matrix $\mathrm{diag}(1, 1/2, 1/2^2, \dots, 1/2^{n-1})$.

However, the probabilities of specific cards ending up in designated places after repeated riffle shufflings are given by the entries of the corresponding power of $M$. By the previous observation, the powers of $M$ can be computed provided we find $P^{-1}$.

## 3. The matrix $P^{-1}$

Remarkably, up to sign, the determinants of the matrices $P$ turn out to be factorials.

Let $v_j^{(n)}$, $j=0,\ldots,n-1$ be the eigenvectors of $M_n$.

LEMMA 3.1. *For $1 \le i \le n-1$ and $0 \le j \le n-1$ we have*

$$v_j^{(n)}(i+1) - v_j^{(n)}(i) = v_{j+1}^{(n+1)}(i+1).$$

*Proof.* Clearly, the statement is true for $j=0$. For $j \ge 1$, we obtain by (2.4) that

$$\begin{aligned} v_j^{(n)}(i+1) - v_j^{(n)}(i) =& (-1)^i \binom{j-1}{i} + (-1)^{n-i+j-1}\binom{j-1}{n-i-1} \\ & - (-1)^{i-1}\binom{j-1}{i-1} - (-1)^{n-i+j}\binom{j-1}{n-i} \\ =& (-1)^i \binom{j}{i} + (-1)^{n-i+j+1}\binom{j}{n-i} \\ =& v_{j+1}^{(n+1)}(i+1). \end{aligned}$$

LEMMA 3.2. $\det(P_n) = (-1)^{\binom{n}{2}} n!$.

*Proof.* The statement is clearly true for $n=1$. Therefore, it suffices to prove that for $n \ge 2$ one has

$$\det(P_n) = (-1)^{n-1} n \det(P_{n-1}). \tag{3.1}$$

Let $A_n$ be the $(n-1)\times(n-1)$ matrix obtained from $P_n$ by deleting the first row and column and let $B_n$ be the $(n-2)\times(n-2)$ matrix obtained from $P_n$ by deleting the first and last rows and the first two columns. By the definition of the eigenvectors $v_i$, the sum of the entries in the first column of $P_n$ is $n$, while the remaining column sums are zero. Therefore, replacing the first row by the sum of all rows in $P_n$ and then expanding on the first row we obtain

$$\det(P_n) = n \det(A_n). \tag{3.2}$$

Since the single nonzero entry in the first column of $A_n$ is the $-1$ in the last row, it follows that $\det(A_n) = (-1)^{n-1}\det(B_n)$. Thus, by (3.2) we obtain

$$\det(P_n) = (-1)^{n-1} n \det(B_n). \tag{3.3}$$

On the other hand, consider the matrix $P_{n-1}$; denote its rows by $R_1,\ldots,R_{n-1}$. For $i=1,\ldots,n-2$, replace $R_i$ by $R_i - R_{i-1}$. Clearly, the only nonzero entry in the first column of the new matrix $P'_{n-1}$ is a 1 in the last row. Moreover, by Lemma 3.1, the matrix obtained from $P'_{n-1}$ by deleting the first row and last column is precisely $B_n$. It follows that $\det(P_{n-1}) = \det(B_n)$, hence (3.3) implies (3.1). $\square$

Denote the $(i,j)$ entry of $P_n^{-1}$ by $q_{ij}^{(n)}$. Since all column sums of $P_n$ are zero except the first one which is equal to $n$, it follows that the entries of the first row of $P_n^{-1}$ are all equal to $1/n$. A simple calculation shows that the vector $\frac{1}{2n-2}(n-1, n-3, n-5, \ldots, -(n-1))$ is orthogonal to all columns of $P_n$ except the second, with which it has scalar product 1. Thus, this vector gives the second row of $P_n^{-1}$. The following result allows us to determine the remaining entries of $P_n^{-1}$ recursively (see also Corollary 3.4).

LEMMA 3.3. *For $3 \le i \le n$ and $1 \le j \le n-1$ we have*

$$q_{ij}^{(n)} - q_{i,j+1}^{(n)} = q_{i-1,j}^{(n-1)}. \tag{3.4}$$

*Proof.* Let $P_n^{(i,j)}$ denote the matrix obtained by deleting row $i$ and column $j$ from $P_n$. We can rewrite (3.4) as

$$(-1)^{i+j} P_n^{(j,i)} - (-1)^{i+j+1} P_n^{(j+1,i)} = (-1)^{i+j-1} \frac{\det(P_n)}{\det(P_{n-1})} P_{n-1}^{(j,i-1)}. \tag{3.5}$$

Let $R_1, \ldots, R_n$ be vectors representing the rows of the matrix $P_n$. For an $n$-vector $v$, denote by $v^{[k,l,\cdots]}$ the vector obtained from $v$ by discarding coordinates $k, l, \ldots$. The left hand side of (3.5) can be expressed as

$$(-1)^{i+j}(P_n^{(j,i)} + P_n^{(j+1,i)}) = (-1)^{i+j} \det \begin{pmatrix} R_1^{[i]} \\ \vdots \\ R_{j-1}^{[i]} \\ R_j^{[i]} + R_{j+1}^{[i]} \\ R_{j+2}^{[i]} \\ \vdots \\ R_n^{[i]} \end{pmatrix}. \tag{3.6}$$

As seen in the proof of Lemma 3.2, the first column sum of the matrix in (3.6) is $n$, and all other column sums are zero. Replacing the first row by the sum of all rows and expanding on the first row, we may rewrite the right hand side of (3.6) as

$$(-1)^{i+j} n \cdot \det \begin{pmatrix} R_2^{[1,i]} \\ \vdots \\ R_{j-1}^{[1,i]} \\ R_j^{[1,i]} + R_{j+1}^{[1,i]} \\ R_{j+2}^{[1,i]} \\ \vdots \\ R_n^{[1,i]} \end{pmatrix}. \tag{3.7}$$

The only nonzero entry in the first column of the matrix in (3.7) is the entry $-1$ in the last row. Expanding on the first column, we obtain by (3.6) and (3.7) that the expression on the left hand side of (3.5) can be written as

$$(-1)^{i+j} P_n^{(j,i)} - (-1)^{i+j+1} P_n^{(j+1,i)} = (-1)^{i+j+n} n \cdot \det \begin{pmatrix} R_2^{[1,2,i]} \\ \vdots \\ R_{j-1}^{[1,2,i]} \\ R_j^{[1,2,i]} + R_{j+1}^{[1,2,i]} \\ R_{j+2}^{[1,2,i]} \\ \vdots \\ R_{n-1}^{[1,2,i]} \end{pmatrix}. \tag{3.8}$$

On the other hand, consider the matrix $P_{n-1}$; denote its row vectors by $L_1, \ldots, L_{n-1}$. By (3.1), the right hand side of (3.5) can be written as

$$(-1)^{i+j+n} n \cdot \det \begin{pmatrix} L_1^{[i-1]} \\ \vdots \\ L_{j-1}^{[i-1]} \\ L_{j+1}^{[i-1]} \\ \vdots \\ L_{n-1}^{[i-1]} \end{pmatrix}. \tag{3.9}$$

Replacing $L_\nu^{[i-1]}$ by $L_\nu^{[i-1]} - L_{\nu-1}^{[i-1]}$ for $\nu = 2, \ldots, n-1$ and expanding on the first column, we conclude from (3.9) that the expression on the right of (3.5) equals

$$(-1)^{i+j+n} n \cdot \det \begin{pmatrix} L_2^{[1,i-1]} - L_1^{[1,i-1]} \\ \vdots \\ L_{j-1}^{[1,i-1]} - L_{j-2}^{[1,i-1]} \\ L_{j+1}^{[1,i-1]} - L_{j-1}^{[1,i-1]} \\ L_{j+2}^{[1,i-1]} - L_{j+1}^{[1,i-1]} \\ \vdots \\ L_{n-1}^{[1,i-1]} - L_{n-2}^{[1,i-1]} \end{pmatrix}. \tag{3.10}$$

However, Lemma 3.1 implies that $L_\nu - L_{\nu-1} = R_\nu^{[1]}$. Since omitting the second and $i$-th coordinates of $R_\nu$ corresponds to discarding the first and $(i-1)$-st coordinates of $R_\nu^{[1]}$, it follows that the matrices appearing in (3.8) and (3.10) are identical. This proves (3.5). $\square$

COROLLARY 3.4. *For $i \geq 3$ and $1 \leq j \leq n$ we have*

$$q_{i1}^{(n)} = \frac{1}{n}\sum_{\nu=1}^{n-1}(n-\nu)q_{i-1,\nu}^{(n-1)} \tag{3.11}$$

$$q_{ij}^{(n)} = q_{i1}^{(n)} - \sum_{\nu=1}^{j-1} q_{i-1,\nu}^{(n-1)}. \tag{3.12}$$

*Proof.* By Lemma 3.3 we obtain

$$\begin{aligned}\sum_{\nu=1}^{j-1} q_{i-1,\nu}^{(n-1)} &= \sum_{\nu=1}^{j-1}\left(q_{i\nu}^{(n)} - q_{i,\nu+1}^{(n)}\right)\\ &= q_{i1}^{(n)} - q_{ij}^{(n)},\end{aligned}$$

which proves (3.12).

On the other hand, since the first column of $P_n$ consists entirely of 1's, the sum of the entries in the $i$-th row of $P_n^{-1}$ is zero for all $i > 1$. Summing both sides of (3.12) for $j = 1, \ldots, n$ we obtain (3.11). □

Lemma 3.5. *For $n \geq 4$ and $3 \leq i \leq n$ we have*

$$\max_j |q_{ij}^{(n)}| \leq \frac{1}{12}\left(\frac{3(n-1)}{2}\right)^{i-2}.$$

*Proof.* The above inequalities are readily checked for $n = 4$ by direct inspection of the entries of $P_4^{-1}$.

Using Lemma 3.3 and the fact that $q_{2j}^{(n)} = (n-2j+1)/(2n-2)$, one readily obtains that the entries in the third row of $P_n^{-1}$ are given by the formula $q_{3j}^{(n)} = [(n-1)/12] - [(j-1)(n-j)/(2n-4)]$. A simple analysis shows that for $n \geq 5$ this quadratic expression in $j$ has absolute value at most $(n-1)/12$, for $j = 1, \ldots, n$. Therefore, the claim is true for $i = 3$.

To complete the proof it suffices to show that, for $n \geq 5$,

$$\max_j |q_{ij}^{(n)}| \leq \frac{3(n-1)}{2}\max_j |q_{i-1,j}^{(n-1)}|. \tag{3.13}$$

By (3.11) we obtain

$$\begin{aligned}|q_{i1}^{(n)}| &\leq \frac{1}{n}\sum_{\nu=1}^{n-1}(n-\nu)|q_{i-1,\nu}^{(n-1)}|\\ &\leq \frac{1}{n}\frac{n(n-1)}{2}\max_j |q_{i-1,j}^{(n-1)}|\\ &= \frac{n-1}{2}\max_j |q_{i-1,j}^{(n-1)}|.\end{aligned}$$

Therefore, (3.12) implies

$$\begin{aligned}|q_{ij}^{(n)}| &\le |q_{i1}^{(n)}| + \sum_{\nu=1}^{j-1} |q_{i-1,\nu}^{(n-1)}| \\ &\le \left(\frac{n-1}{2} + n - 1\right) \max_j |q_{i-1,j}^{(n-1)}|,\end{aligned}$$

which proves (3.13). □

## 4. The proof of Theorem 1.1

We return now to the guessing problem described in the Introduction. Since the guesser is given no feedback, his best strategy is to guess at each step $j$ the most likely card to end up in position $j$ after $k$ riffle shuffles, i.e., his guess should be the index of the row containing the largest element of the $j$-th column of $M^k$.

The argument used to prove (2.3) also shows that $(M^k)_{ij} = (M^k)_{n-i+1,n-j+1}$. Therefore, it suffices to show that the largest entry in each of the first $n$ columns of $(M_{2n})^k$ lies in the first row: this implies that the largest entry in each of the remaining columns is the one in the last row.

For the sake of notational simplicity, let $q_{ij}$ stand for the $(i, j)$ entry of $P_{2n}^{-1}$ (this was previously denoted by $q_{ij}^{(2n)}$). Let $P_{2n} = (p_{ij})_{1\le i,j\le 2n}$. By the remark at the end of Section 2, the powers of $M = M_{2n}$ are given by

$$M^k = P_{2n} \cdot \operatorname{diag}(1, 1/2^k, 1/2^{2k}, \ldots, 1/2^{(2n-1)k}) \cdot P_{2n}^{-1}.$$

Expanding the product on the right hand side we deduce that the $(l, j)$-entry of $M^k$ is given by

$$(M^k)_{lj} = \sum_{i=1}^{2n} p_{li} q_{ij}/2^{(i-1)k}. \tag{4.1}$$

Since $p_{12} = 1$ and $p_{l2} \le 0$ for $l > 1$, we obtain using $p_{1i} = 1$, $q_{1j} = 1/(2n)$, and the formula expressing the $q_{2j}$'s that for $1 \le j \le n$

$$\begin{aligned}(M^k)_{1j} &= \frac{1}{2n} + \frac{2n-2j+1}{4n-2}\frac{1}{2^k} + \sum_{i=3}^{2n} \frac{q_{ij}}{2^{(i-1)k}} \\ &\ge \frac{1}{2n} + \frac{2n-2j+1}{4n-2}\frac{1}{2^k} - \sum_{i=3}^{2n} \frac{|q_{ij}|}{2^{(i-1)k}} \end{aligned}\tag{4.2}$$

$$\begin{aligned}(M^k)_{lj} &= \frac{1}{2n} + \frac{2n-2j+1}{4n-2}\frac{p_{l2}}{2^k} + \sum_{i=3}^{2n} \frac{p_{li}q_{ij}}{2^{(i-1)k}} \\ &\le \frac{1}{2n} + \sum_{i=3}^{2n} \frac{|p_{li}||q_{ij}|}{2^{(i-1)k}}, \quad \text{for } l > 1.\end{aligned}\tag{4.3}$$

By the definition of the entries of $P$, it follows that $|p_{li}| \leq 2^{i-1} - 1$ for $i \geq 2$. Therefore, by (4.2) and (4.3), to prove part (a) of Theorem 1.1 it suffices to show that for $k \geq 2\log_2(2n) + 1$ and $1 \leq j \leq n$ we have

$$\frac{2n - 2j + 1}{4n - 2} \frac{1}{2^k} > \sum_{i=3}^{2n} \frac{|q_{ij}|}{2^{(i-1)(k-1)}}. \tag{4.4}$$

The statement of Theorem 1.1(a) is easily checked directly for $n = 1$. For $n \geq 2$, we deduce from Lemma 3.5 that

$$\begin{aligned}\sum_{i=3}^{2n} \frac{|q_{ij}|}{2^{(i-1)(k-1)}} &\leq \frac{1}{12} \sum_{i=3}^{2n} \frac{(3n)^{i-2}}{2^{(i-1)(k-1)}} \\ &= \frac{1}{12} \frac{1}{2^{k-1}} \sum_{i=3}^{2n} \left( \frac{3n}{2^{k-1}} \right)^{i-2}. \end{aligned} \tag{4.5}$$

Let $k - 1 = 2\log_2(3n) + d$ and write $d = \log_2 \alpha$. Then $2^{k-1} = \alpha(3n)^2$ and (4.5) yields

$$\begin{aligned}\sum_{i=3}^{2n} \frac{|q_{ij}|}{2^{(i-1)(k-1)}} &\leq \frac{1}{12} \frac{1}{\alpha(3n)^2} \sum_{i=3}^{2n} \left( \frac{1}{3\alpha n} \right)^{i-2} \\ &< \frac{1}{12} \frac{1}{\alpha(3n)^2} \frac{1}{3\alpha n - 1} \end{aligned} \tag{4.6}$$

(where at the second inequality we assume $3\alpha n > 1$). On the other hand, the left hand side of (4.4) is minimum for $j = n$, when it equals $1/((4n-2)2^k) = 1/(4\alpha(2n-1)(3n)^2)$. Therefore, (4.6) implies that (4.4) holds whenever

$$\frac{1}{4\alpha(2n-1)(3n)^2} \geq \frac{1}{12\alpha(3n)^2(3\alpha n - 1)}.$$

A simple calculation shows that this is equivalent to $(9\alpha - 2)n \geq 2$, which is true for all $n$ as long as $\alpha \geq 4/9$ (this implies $3\alpha n > 1$, so the last inequality in (4.6) is true for all such $\alpha$). In view of our choice of $k$, the latter condition is equivalent to $k - 1 \geq 2\log_2(2n)$, thus proving part (a) of Theorem 1.1.

To complete the proof, we show that the conditions stated in part (b) of Theorem 1.1 imply $(M^k)_{2n} > (M^k)_{1n}$, i.e., that after $k$ shuffles card 2 is more likely to be in position $n$ than is card 1.

Using the formulas for the entries $q_{2i}$ and $q_{3i}$ given in the proof of Lemma 3.5, we obtain that $q_{2n} = 1/(4n-2)$ and $q_{3n} = -(n+1)/12$. Therefore, (4.1) yields

$$
\begin{aligned}
(M^k)_{1n} &= \frac{1}{2n} + \frac{1}{4n-2}\frac{1}{2^k} - \frac{n+1}{12}\frac{1}{4^k} + \sum_{i=4}^{2n} \frac{q_{in}}{2^{(i-1)k}} \\
&\leq \frac{1}{2n} + \frac{1}{4n-2}\frac{1}{2^k} - \frac{n+1}{12}\frac{1}{4^k} + \sum_{i=4}^{2n} \frac{|q_{in}|}{2^{(i-1)k}} \qquad (4.7) \\
(M^k)_{2n} &= \frac{1}{2n} + \frac{n+1}{12}\frac{1}{4^k} + \sum_{i=4}^{2n} \frac{p_{2i}q_{in}}{2^{(i-1)k}} \\
&\geq \frac{1}{2n} + \frac{n+1}{12}\frac{1}{4^k} - \sum_{i=4}^{2n} \frac{(i-1)|q_{in}|}{2^{(i-1)k}} \qquad (4.8)
\end{aligned}
$$

(in (4.8) we used that $|p_{2i}| \leq i-1$).

By (4.7) and (4.8), to prove the inequality $(M^k)_{2n} > (M^k)_{1n}$ it suffices to show that

$$
\frac{n+1}{6}\frac{1}{4^k} - \frac{1}{4n-2}\frac{1}{2^k} > \sum_{i=4}^{2n} \frac{i|q_{in}|}{2^{(i-1)k}}. \qquad (4.9)
$$

Since $k = c\log_2(2n)$ we can write $2^k = \alpha(3n)^c$, where $\alpha = (2/3)^c$. Using Lemma 3.5 we obtain (for $n \geq 2$)

$$
\begin{aligned}
\sum_{i=4}^{2n} \frac{i|q_{in}|}{2^{(i-1)k}} &\leq \frac{1}{12 \cdot 2^k} \sum_{i=4}^{2n} i \left(\frac{3n}{2^k}\right)^{i-2} \\
&= \frac{1}{12\alpha(3n)^c} \sum_{i=4}^{2n} i \left(\frac{1}{\alpha(3n)^{c-1}}\right)^{i-2}. \qquad (4.10)
\end{aligned}
$$

To estimate the last sum in (4.10), notice that the ratio between the $(i+1)$-st and $i$-th terms in this sum is $(i+1)/(i\alpha(3n)^{c-1})$. Since $c > 1$, there exists some positive integer $n_1(c)$ such that this ratio is at most $1/2$ for all $n \geq n_1(c)$. It follows from (4.10) that for all $n \geq n_1(c)$ we have

$$
\begin{aligned}
\sum_{i=4}^{2n} \frac{i|q_{in}|}{2^{(i-1)k}} &\leq \frac{1}{12\alpha(3n)^c} \frac{4}{\alpha^2(3n)^{2c-2}} \sum_{i=4}^{2n} 1/2^{i-4} \\
&< \frac{2}{3}\frac{1}{\alpha^3(3n)^{3c-2}}. \qquad (4.11)
\end{aligned}
$$

By using $2^k = \alpha(3n)^c$ on the left hand side of (4.9), we deduce from (4.11) that (4.9) is implied (for $n \geq n_1(c)$) by the inequality

$$
\frac{n+1}{6}\frac{1}{\alpha^2(3n)^{2c}} \geq \frac{1}{4n-2}\frac{1}{\alpha(3n)^c} + \frac{2}{3}\frac{1}{\alpha^3(3n)^{3c-2}}. \qquad (4.12)
$$

The expression on the left is $\Theta(n^{1-2c})$, while the two terms on the right are $\Theta(n^{-1-c})$ and $\Theta(n^{2-3c})$, respectively. Therefore, as long as $1-2c > -1-c$ and $1-2c > 2-3c$, there exists some positive integer $n_2(c)$ such that (4.12) holds for all $n \geq n_2(c)$. Since these two inequalities for $c$ are equivalent to our assumption $1 < c < 2$, it follows that (4.9) holds for all $n \geq \max(n_1(c), n_2(c))$ and the proof is complete.

Remark. Numerical evidence strongly suggests that the statement of Theorem 1.1(b) is also true for $0 < c \leq 1$. However, the above method does not seem to apply to this case, essentially because the estimates (4.7), (4.8), and (4.10) are not sharp enough for small $k$.

## 5. A well-mixed deck

It is natural to ask how many shuffles of a deck of $n$ cards are needed to obtain a well-mixed deck. The standard way of measuring how well the deck is mixed after $k$ shuffles is to consider the total variation distance from the resulting probability distribution to the uniform distribution. This approach is used in [**3**], where it is proved that this total variation distance drops abruptly around the value $k = (3/2)\log_2 n$ from being very close to 1 to being very close to 0.

Alternatively, as mentioned in [**3**], one can measure how well the deck is mixed by means of a card guessing problem (the problem considered in [**3**] is the one in which the guesser is provided complete feedback, i.e., he is showed each card after guessing at it; we consider here the no-feedback case). Notice that if the deck is perfectly mixed (i.e., all orderings are equally likely), then for all guessing strategies the expected number of correct guesses equals 1. Now, suppose the deck has been given $k$ riffle shuffles (the initial ordering of the deck is known to the guesser). Then it is natural to measure how well the deck is mixed by $|E^k(n) - 1|$, where $E^k(n)$ is the expected number of correct guesses when the best strategy is used.

Let $n$ be even. As a consequence of Theorem 1.1(a), once $k \geq 2\log_2 n + 1$, the number of correct guesses under the best strategy can be at most 2. Therefore, we have $E^k(n) \leq 2$. Thus, since the best guessing strategy yields only a gain of at most 1 over the case of the uniform distribution, one can say that the deck is well-mixed (this is indeed a small gain, since by Corollary 5.5(b), $E^1(n) = \Theta(\sqrt{n})$).

In the complete feedback case, for a deck chosen uniformly at random, it is clear that the best strategy is to guess at each step a card known to be in the deck, and the expected number of correct guesses under this strategy is $h_n := 1 + (1/2) + \cdots + (1/n)$. Let $F^k(n)$ denote the expected number of correct guesses under the best strategy for the complete feedback problem with an $n$-card deck shuffled $k$ times. As indicated in [**3**], numerical evidence suggests that, once $k$ is sufficiently large so that the deck is well-mixed, each additional shuffle cuts the difference $F^k(n) - h_n$ roughly in half. In this section we prove (see Corollary 5.2) that a similar phenomenon occurs in the no-feedback case.

Proposition 5.1. *For $k \geq 2\log_2(2n) + 1$,*

$$E^k(2n) = 1 + \frac{n^2}{2n-1}\frac{1}{2^k} + 2\sum_{i=2}^{n}\left(q_{2i+1,1}^{(2n+1)} - q_{2i+1,n+1}^{(2n+1)}\right)/2^{(2i-1)k}. \tag{5.1}$$

*Proof.* Let $M = M_{2n}$ be the position matrix for the $2n$-card deck. By Theorem 1.1(a), in the case under consideration we have

$$E^k(2n) = (M^k)_{11} + \cdots + (M^k)_{1n} + (M^k)_{2n,n+1} + \cdots + (M^k)_{2n,2n}. \tag{5.2}$$

Using $p_{1i} = 1$ we obtain by (4.1) that

$$(M^k)_{1m} = \sum_{i=1}^{2n} \frac{q_{im}^{(2n)}}{2^{(i-1)k}},$$

$m = 1, \ldots, n$. By the central symmetry of the matrix $M^k$ we deduce therefore from (5.2) that

$$\begin{aligned} E^k(2n) &= 2 \sum_{m=1}^{n} \sum_{i=1}^{2n} \frac{q_{im}^{(2n)}}{2^{(i-1)k}} \\ &= 2 \sum_{i=1}^{2n} \frac{1}{2^{(i-1)k}} \sum_{m=1}^{n} q_{im}^{(2n)}. \end{aligned} \tag{5.3}$$

However, since the columns of the matrix $P$ are alternately symmetric and antisymmetric with respect to the horizontal symmetry axis of $P$, it follows that the rows of $P^{-1}$ are alternately symmetric and antisymmetric with respect to the vertical symmetry axis of $P^{-1}$. Since the sum of the entries in each row of index at least 2 in $P^{-1}$ is zero, it follows that the summand in the last sum on $i$ of (5.3) is zero unless $i$ is even. Using (3.12) and replacing $q_{2m}^{(2n)} = (2n - 2m + 1)/(4n - 2)$ in (5.3) we obtain the formula in the statement of the Lemma. $\square$

Corollary 5.2. *For any $1 < a < 2$ there exists a positive integer $k_a$ such that for all $n$ and for all $k \geq 2\log_2(2n) + k_a$ we have $E^{k+1}(2n) - 1 \leq (E^k(2n) - 1)/a$.*

*Proof.* By (5.1), the statement holds in the case $n = 1$ with $k_a = 1$. Assume therefore $n \geq 2$. Denote by $S$ the sum on the right hand side of (5.1). By Lemma 3.5 we have

$$\begin{aligned} |S| &\leq \sum_{i=2}^{n} \left( |q_{2i+1,1}^{(2n+1)}| + |q_{2i+1,n+1}^{(2n+1)}| \right) / 2^{(2i-1)k} \\ &\leq 2 \sum_{i=2}^{n} \frac{1}{12} \left( \frac{3n}{2^k} \right)^{2i-1} \\ &\leq \frac{1}{6} \left( \frac{3n}{2^k} \right)^3 \left( 1 - \left( \frac{3n}{2^k} \right)^2 \right)^{-1}. \end{aligned} \tag{5.4}$$

Let $2^k = \alpha(3n)^2$. For $\alpha \geq 1$, (5.4) implies

$$
\begin{aligned}
2|S| &\le \frac{1}{3}\frac{1}{2^{3k/2}}\left(\frac{3n}{2^{k/2}}\right)^3\left(1-\left(\frac{3n}{2^k}\right)^2\right)^{-1} \\
&= \frac{1}{3}\frac{1}{2^{3k/2}}\frac{1}{\alpha^{3/2}}\left(1-\left(\frac{1}{3\alpha n}\right)^2\right)^{-1} \\
&\le 2^{-3k/2},
\end{aligned} \tag{5.5}
$$

for all $n$. By (5.1) and (5.5) we obtain

$$
\begin{aligned}
E^k(2n)-1 &\ge \frac{n^2}{2n-1}\frac{1}{2^k} - 2^{-3k/2} \\
E^{k+1}(2n)-1 &\le \frac{n^2}{2n-1}\frac{1}{2^{k+1}} + 2^{-3(k+1)/2}.
\end{aligned}
$$

Therefore,

$$
\begin{aligned}
(E^k(2n)-1) - a(E^{k+1}(2n)-1) &\ge \frac{1-a/2}{2^k}\frac{n^2}{2n-1} - 2^{-3k/2} - a2^{-3(k+1)/2} \\
&\ge \frac{1-a/2}{2^k}\frac{n^2}{2n-1} - (1+a)2^{-3k/2}.
\end{aligned} \tag{5.6}
$$

Since we are assuming $n \ge 2$, replacing $2^k = \alpha(3n)^2$ we obtain that the right hand side of (5.6) is nonnegative whenever $4\sqrt{\alpha} \ge (1+a)/(2-a)$. This proves the Corollary. $\square$

Remark 5.3. Using Lemma 2.1, one can work out explicitly the value of $E^1(n)$, i.e., the expected number of correct guesses under the best strategy when the deck is given a single riffle shuffle (Lemma 5.4 gives the best strategy; Corollary 5.5 gives $E^1(n)$ for $n$ even).

Lemma 5.4. *In the case of a single riffle shuffle, a strategy that maximizes the expected number of correct guesses is to guess, in order,* $1, 2, 2, 3, 3, 4, 4, 5, 5\dots$ *until we reach the middle of the deck, and then guess so that the rest of the guessing sequence, read backwards, is* $n, n-1, n-1, n-2, n-2, \cdots$.

*Proof.* By Lemma 2.1, the entries of the $k$-th column of the position matrix $M_n$ are $2^{-n}$ times the following:

$$
\begin{aligned}
&2^{n-k}\binom{k-1}{k-1}, 2^{n-k}\binom{k-1}{k-2}, \cdots, 2^{n-k}\binom{k-1}{1}, \\
&2^{n-k}+2^{k-1}, \\
&2^{k-1}\binom{n-k}{1}, 2^{k-1}\binom{n-k}{2}, \cdots, 2^{k-1}\binom{n-k}{n-k}.
\end{aligned} \tag{5.7}
$$

Since the best guess at the card in position $k$ is the index of the row containing the largest entry of the $k$-th column of $M_n$, all we need to do is determine the largest of the numbers (5.7).

Clearly, $A := 2^{n-k}\binom{k-1}{\lfloor (k-1)/2\rfloor}$ and $B := 2^{k-1}\binom{n-k}{\lfloor (n-k)/2\rfloor}$ are the largest of the first $k-1$ and last $n-k$ numbers in (5.7), respectively. Therefore, it suffices to compare the largest of these two numbers to $C := 2^{n-k} + 2^{k-1}$.

For $i \geq 1$, define $a_i := \binom{i}{\lfloor i/2\rfloor}/2^i$. Considering separately the cases of even or odd $i$, it is straightforward to check that $a_{i+1}/a_i \leq 1$ for all $i \geq 1$. It follows that for $k \leq \lfloor (n+1)/2\rfloor$ we have $A \geq B$. Furthermore, it is clear that for $3 \leq k \leq \lfloor (n+1)/2\rfloor$ we also have $A \geq C$. On the other hand, for $k \leq 2$ the largest of the numbers (5.7) is $C$. This proves the statement of the Lemma. □

Corollary 5.5. *(a) For all $n \geq 1$ we have*

$$E^1(2n) = \frac{3}{2^{2n-1}} + \sum_{i=0}^{n-1} \frac{1}{2^i}\binom{i}{\lfloor i/2\rfloor}.$$

*(b) $E^1(2n) \sim \sqrt{\frac{8}{\pi}}\sqrt{n}$.*

*Proof.* Part (a) follows directly from Lemmas 5.4 and 2.1. To obtain (b), note that Stirling's formula implies that $\binom{2i}{i}/2^{2i} \sim 1/\sqrt{\pi i}$ for large $i$. Moreover, an immediate calculation shows that $\binom{2i-1}{i-1}/2^{2i-1} = \binom{2i}{i}/2^{2i}$, for all $i$. Part (b) follows now from the fact that $\sum_{i=1}^n 1/\sqrt{i} \sim 2\sqrt{n}$. □

**Note.** One can generalize dovetail shuffling as follows (see e.g. [**3**]). Consider a deck of cards and let $a \geq 2$ be an integer. An *$a$-shuffle* consists of (1) cutting the deck by selecting $a-1$ cutting places at random according to the multinomial distribution and (2) interleaving the $a$ resulting decks at random, according to the uniform distribution.

All the results discussed in this paper can be extended to $a$-shuffles. More precisely, let $M_n^{(a)}$ denote the $n\times n$ matrix whose $(i,j)$ entry is the probability that card $i$ goes to position $j$ after an $a$-shuffle. Then it turns out that the eigenvalues of $M_n^{(a)}$ are $1, 1/a, \ldots, 1/a^{n-1}$, and, remarkably, the eigenvectors are *the same* as in the case $a = 2$.

This can be proved as follows. Let $R^{(a)} = R_n^{(a)}$ be the matrix whose rows and columns are indexed by permutations on $n$ elements and whose $(\sigma,\tau)$ entry is the probability that a deck in order $\sigma$ ends up in order $\tau$ after an $a$-shuffle. Regarding $R^{(a)}$ as a linear transformation and considering a suitable change of basis, one can see that $R^{(a)}$ is similar to a block-diagonal matrix having $M^{(a)}$ as one of the blocks (indeed, consider any basis containing the $n$ vectors $\sum_{\sigma:\sigma^{-1}(1)=1}\sigma, \ldots, \sum_{\sigma:\sigma^{-1}(1)=n}\sigma$; these vectors span an invariant subspace whose matrix is $M^{(a)}$).

Since $R^{(a)}R^{(b)} = R^{(ab)}$ (see e.g. [**3**]), it follows from the previous paragraph that $M^{(a)}M^{(b)} = M^{(ab)}$. Let $D = \mathrm{diag}(1, 1/2, \ldots, 1/2^{n-1})$ and let $P$ be the matrix whose columns are the eigenvectors of $M = M^{(2)}$. Then by Theorem 2.2 we obtain

$$M^{(2^k)} = \left(M^{(2)}\right)^k = P^{-1}D^kP,$$

which implies that our claim about the eigenvalues and eigenvectors of $M^{(a)}$ is true for $a = 2^k$, $k \geq 1$.

However, this implies our claim for arbitrary $a$. Indeed, we know by [**3**, Theorem 3] that

$$R^{(a)}_{\mathrm{id},\pi} = \frac{1}{a^n} \binom{n + a - r(\pi)}{n},$$

where $r(\pi)$ is the number of rising sequences of $\pi$. It follows that

$$M^{(a)}_{i,j} = \frac{1}{a^n} \sum_{\pi : \pi^{-1}(i) = j} \binom{n + a - r(\pi)}{n}.$$

Let $v_m$ be the $m$-th column of $P$. Then the coordinates of the vector $a^{(m-1)} M^{(a)} \cdot v_m - v_m$ are polynomials in $a$ that vanish at $a = 2^k$, $k \geq 1$, and are therefore identically zero. This completes the proof.

**Acknowledgments.** I would like to thank Phil Hanlon for suggesting the problem addressed in this paper and for helpful discussions. I wish to thank Persi Diaconis for his interest and for useful references. The form of the eigenvectors of the position matrix was first conjectured by Patrick Bidigaire. I am grateful to the Associate Editor and to the referee for their careful reading of the manuscript.

## References

[**1**] D. Aldous, Random walks on finite groups and rapidly mixing Markov chains, "Séminaire de Probabilités XVII," 243–297, Lecture notes in Math. **986**, Springer, New York, 1983.

[**2**] D. Aldous and P. Diaconis, Shuffling cards and stopping times, *Amer. Math. Monthly* **93** (1986), 333–348.

[**3**] D. Bayer and P. Diaconis, Trailing the dovetail shuffle to its lair, *Ann. Appl. Probab.* **2** (1992), 294–313.

[**4**] P. Diaconis, Group representations in probability and statistics, IMS, Hayward, California, 1988.

[**5**] P. Diaconis, M. McGrath, and J. Pitman, Riffle shuffles, cycles, and descents, *Combinatorica* **15** (1995), 11–29.

[**6**] S. P. Lalley, Cycle structure of riffle shuffles, *Ann. Probab.* **24** (1996), 49–73.

[**7**] B. Mann, How many times should you shuffle a deck of cards, in "Topics in contemporary probability and its applications," J. Laurie Snell, Ed., CRC Press, Boca Raton, 1995, 261–289.

[**8**] J. Riordan, "Combinatorial identities," Robert E. Krieger Publishing Co., Huntington, N.Y., 1979.