A Strong Uniform Time for Random Transpositions

by

Peter Matthews
Purdue University

Technical Report #86-23

Department of Statistics
Purdue University

June 1986

A Strong Uniform Time for Random Transpositions

by

Peter Matthews
Purdue University

Summary

A random permutation of N items generated by a sequence of K random transpositions is considered. The method of strong uniform times is used to give an upper bound on the variation distance between the distributions of the random permutation generated and a uniformly distributed permutation. The strong uniform time is also used to find the asymptotic distribution of the number of fixed points of the generated permutation. This is used to give a lower bound on the same variation distance. Together these bounds give a striking demonstration of the threshold phenomenon in the convergence of rapidly mixing Markov chains to stationarity.

1. Introduction and Results

Diaconis and Shashahani (1981) studied the following process. Consider a deck of N cards labelled $1, 2, \ldots, N$. Two cards, L_1 and R_1, are chosen uniformly and independently by left and right hands and transposed if they differ. This step is repeated independently many times. After a large number K of iterations the cards will be well mixed; the distribution, denoted μ^{K*}, of the resulting permutation, denoted π_K, will be close to the uniform distribution, denoted U, on the symmetric group $Sym(N)$. Interest in Diaconis and Shashahani (1981) and this paper lies in the non-asymptotics of the convergence to uniformity.

More formally, for two probability distributions μ and ν on a finite set $\mathcal{A}$, the variation distance between μ and ν is

$$d(\mu, \nu) = \max_{A \subset \mathcal{A}} |\mu(A) - \nu(A)|.$$

For this process $d(\mu^{k*}, U) \to 0$ as $k \to \infty$. Diaconis and Shashahani (1981) showed that most of the action happens near $k = \frac{1}{2} N \log N$ and that the natural approach to this problem is to take $K = \frac{1}{2} N \log N + cN$ for some constant c and study

$$d_c = d(\mu^{K*}, U), \tag{1.1}$$

the dependence on N being suppressed. In what follows K and c will always be related in this way, and any asymptotics will hold c fixed and let N, and hence K, go to infinity.

Diaconis and Shashahani (1981) considered the process as a random walk on the symmetric group and, using some hard fourier analysis, showed that there is a constant b such that for all $N \geq 10$,

$$d_c \leq b\, e^{-2c}. \tag{1.2}$$

They credit to Charles Stein an argument showing

$$d_c \geq \frac{1}{e} - e^{-e^{-2c}} + o(1). \tag{1.3}$$

Facts (1.2) and (1.3) together imply that d_c is large for c much less than 0 and drops quickly for $c > 0$. The variation distance drops from essentially 1 to essentially 0 in an interval of width $0(N)$ around $\frac{1}{2}N \log N$. This is an example of the threshold phenomenon discussed in Aldous (1983) and Aldous and Diaconis (1986).

This paper will give more precise bounds via the probabilistic method of strong uniform times. For this shuffling process a strong uniform time is a stopping time T, typically randomized, such that

$$P(\pi_k = \pi | T \leq k) = \frac{1}{N!} \text{ for all } k \text{ and } \pi.$$

In words, the conditional distribution of π_k given that T has come to pass is exactly uniform. The main use of strong uniform times is that for any strong uniform time T,

$$d(\mu^{k*}, U) \leq P(T > k) \text{ for all } k. \tag{1.4}$$

Diaconis (1986) discusses the use of strong uniform times.

Broder (1985) developed the method of card checking for constructing strong uniform times. He gave a strong uniform time T for the problem of random transpositions with mean $E(T) = 2N \log N(1 + o(1))$ and variance $\sigma^2(T) = 0(N^2)$. This plus Chebychev's inequality shows that $d(\mu^{k*}, U)$ must be small once k is much bigger than $2N \log N$, a weaker result than (1.2).

Here an improved strong uniform time is given. Its distribution is calculated and (1.4) gives

$$d_c \leq 1 - e^{-(2e)e^{-2c}} + o(1). \tag{1.5}$$

The strong uniform time is also used to give a lower bound on d_c. Let $|Fix_c|$ denote the number of fixed points (cards in their original positions) of π_K. It is shown that

$$|Fix_c| \xrightarrow{dist} \text{Poisson } (1 + e^{-2c}). \tag{1.6}$$

The classic problème des rencontres (Riordan, 1978) has as its answer the fact that the number of fixed points of a uniformly distributed permutation has asymptotically a Poisson (1) distribution. By breaking $Sym(N)$ into classes according to number of fixed points, we see

$$d_c > d(\text{Poisson } (1 + e^{-2c}), \text{ Poisson } (1)) + o(1). \tag{1.7}$$

The following table gives the asymptotic lower and upper bounds on d_c for various values of c.

c	$d(\text{Poisson}\,(1+e^{-2c}),\ \text{Poisson}\,(1))$	$1-e^{-(2e)e^{-2c}}$
-2	$1-e^{-21}$	$1-e^{-297}$
-1.5	$.9969 = 1-e^{-5.8}$	$1-e^{-109}$
-1	.949	$1-e^{-40}$
$-.5$	.64	$1-e^{-15}$
0	.33	.996
.5	.13	.86
1	$.050 = e^{-3}$	.52
1.5	$.018 = e^{-4}$	.24
2	$.0067 = e^{-5}$	.095
2.5	$.0025 = e^{-6}$	.036
3	$.0009 = e^{-7}$	.013
4	e^{-9}	$.0018 = e^{-6.3}$
5	e^{-11}	$.00025 = e^{-8.3}$

The table shows that the variation distance drops drastically, from essentially 1 to essentially 0, in an interval of length about $2N$ near $\frac{1}{2}N \log N$. As $c \longrightarrow \infty$ the bounds differ by a factor of $2e^2$.

The remainder of this article is organized as follows. Section 2 gives the strong uniform time. Section 3 works with its generating function and gives the upper bound (1.5). Section 4 gives (1.6) and hence the lower bound (1.7). Finally Section 5 gives a proof that the stopping time used is a strong uniform time.

Acknowledgement. I would like to thank Persi Diaconis for many helpful discussions.

2. The Strong Uniform Time

At each step k of the shuffling process two cards, L_k and R_k, are chosen independently and uniformly and switched if they differ. Formally, the random transposition (L_k, R_k) is performed. The strong uniform time involves "checking" cards as they are moved; the first time all cards are checked is the strong uniform time. At the start no cards are checked. Let $\lceil x \rceil$ denote the least integer greater than or equal to x. There will be two different ways for cards to be checked, according to whether the number of cards previously checked is $< \lceil N/3 \rceil$ or $\geq \lceil N/3 \rceil$.

First suppose $n < \lceil N/3 \rceil$ cards are checked after time $k-1$. Then at the kth move, if both L_k and R_k are unchecked, check R_k. Let T_n denote the time taken to check n cards and $T_0 = 0$. Then for $n \leq \lceil N/3 \rceil, T_n - T_{n-1}$ is the time taken to check the nth card after

$n-1$ are checked. $T_n - T_{n-1}$ has a geometric distribution with probability of success

$$p_n = \left(\frac{N-(n-1)}{N}\right)^2. \tag{2.1}$$

Further $T_1 - T_0, T_2 - T_1, \ldots, T_{\lceil N/3 \rceil} - T_{\lceil N/3 \rceil - 1}$ are independent.

The intuition for this part of the strong uniform time is as follows. One way to build a random permutation is to take a list of cards and a list of slots, choose one of each at random, place the card in the slot, choose another pair, etc. The first part of the card checking procedure is an attempt to embed this process in the shuffling process. We think of the right hand as choosing a candidate card and of the left hand as choosing a candidate slot. If both are available, the pair is accepted. Otherwise it is rejected. Section 5 will verify that this is essentially how this part of the card checking procedure works.

Once $\lceil N/3 \rceil$ cards are checked a more complex procedure is used. This procedure is essentially Broder's original algorithm, but modified to check cards twice as fast. Recall that the cards are labelled $1, 2, \ldots, N$. If $n - 1 \geq \lceil N/3 \rceil$ cards are checked, assume their labels are $\ell_1 < \ell_2 < \ldots < \ell_{n-1}$. List all possible (L, R) pairs made up of these cards in dictionary order;

$$(\ell_1, \ell_1), (\ell_1, \ell_2), \ldots, (\ell_1, \ell_{n-1}), (\ell_2, \ell_1), \ldots, (\ell_{n-1}, \ell_{n-1}). \tag{2.2}$$

Also list the unchecked cards in dictionary order; $u_1 < u_2 < \ldots < u_{N-n+1}$. For $i = 1, 2, \ldots, N - n + 1$, check card u_i if either

(2.3)
- *a)* $(L, R) = (u_i, u_i)$
- *b)* One hand chooses u_i and the other hand chooses a checked card
- *c)* The ith (L, R) pair in (2.2) is chosen.

For $N \geq 4$ it is easy to check that (2.2) will contain at least $N - \lceil N/3 \rceil$ pairs. For $N \leq 3$ the procedure must be modified slightly. Also note that at most one card can be checked at each step and that (2.3)c is the only way a card can be checked without being touched by either hand.

Again let T_n be the time taken to check n cards. For $n > \lceil N/3 \rceil$ $T_n - T_{n-1}$ has a geometric distribution with probability of success

$$p_n = \frac{2n(N-n+1)}{N^2}. \tag{2.4}$$

Further $(T_1 - T_0), (T_2 - T_1), \ldots, (T_N - T_{N-1})$ are independent.

The intuition for this part of the card checking procedure is that it is equivalent to another method of building a random permutation. If a partial permutation has $n - 1$ randomly ordered cards, then there are n slots in which a new card could be added. This card checking procedure tries to add new cards to the partial permutation by putting each

new card into the available slots with uniform probability. That this is correct and that the two procedures mesh together properly will be verified in Section 5.

3. Generating Functions and the Upper Bound

Recall T_n is the first time n cards are checked. As a special case T_N is the strong uniform time of interest. The moment generating function of T_N will give its distribution and hence an upper bound via (1.4). The generating functions of T_n for $n = N - 0(1)$ are needed in Section 4 and will also be given here.

A geometric random variable T with probability of success p has moment generating function

$$E\, e^{tT} = \frac{p\, e^t}{1-(1-p)e^t} \quad \text{for} \quad t < -\log\,(1-p).$$

Thus for $n > \lceil N/3 \rceil$, by (2.1) and (2.4), T_n has moment generating function

$$E\, e^{tT_n} = \prod_{m=1}^{\lceil N/3 \rceil} \frac{\left(\frac{N-m+1}{N}\right)^2 e^t}{1-\left(1-\left(\frac{N-m+1}{N}\right)^2\right) e^t} \quad \times$$

$$\prod_{m=\lceil N/3 \rceil+1}^{n} \frac{\frac{2m(N-m+1)}{N^2} e^t}{1-\left(1-\frac{2m(N-m+1)}{N^2}\right) e^t}$$

$$\text{for } t < -\log\left(1-\frac{2n(N-n+1)}{N^2}\right).$$

This is

$$\prod_{m=1}^{\lceil N/3 \rceil} \frac{(N-m+1)^2}{\left(N\left[1+\sqrt{1-e^{-t}}\right]-m+1\right)\left(N\left[1-\sqrt{1-e^{-t}}\right]-m+1\right)} \quad \times \prod_{m=\lceil N/3 \rceil+1}^{n}$$

$$\frac{m(N-m+1)}{\left(\frac{N+1}{2}+\frac{1}{2}\sqrt{(N+1)^2-2N^2(1-e^{-t})}-m\right)\left(m-\frac{N+1}{2}+\frac{1}{2}\sqrt{(N+1)^2-2N^2(1-e^{-t})}\right)}.$$

In terms of gamma functions this is

$$\left(\frac{\Gamma(N+1)}{\Gamma(N-\lceil N/3 \rceil+1)}\right)^2$$

$$\times \quad \frac{\Gamma(N[1+\sqrt{1-e^{-t}}]-\lceil N/3 \rceil+1)}{\Gamma(N[1+\sqrt{1-e^{-t}}]+1)} \frac{\Gamma(N[1-\sqrt{1-e^{-t}}]-\lceil N/3 \rceil+1)}{\Gamma(N[1-\sqrt{1-e^{-t}}]+1)}$$

$$\times \quad \frac{\Gamma(n+1)}{\Gamma(\lceil N/3 \rceil+1)} \frac{\Gamma(\frac{N+1}{2}+\frac{1}{2}\sqrt{(N+1)^2-2N^2(1-e^{-t})}-n)}{\Gamma(\frac{N+1}{2}+\frac{1}{2}\sqrt{(N+1)^2-2N^2(1-e^{-t})}-\lceil N/3 \rceil)}$$

$$\times \quad \frac{\Gamma(N+1-\lceil N/3\rceil)}{\Gamma(N+1-n)} \frac{\Gamma(\lceil N/3\rceil+1-\frac{N+1}{2}+\frac{1}{2}\sqrt{(N+1)^2-2N^2(1-e^{-t})})}{\Gamma(n+1-\frac{N+1}{2}+\frac{1}{2}\sqrt{(N+1)^2-2N^2(1-e^{-t})})}.$$

Let $s = \frac{Nt}{2}$ and $J = N - n$. Then straightforward use of Stirling's formula and Taylor expansions shows that for J fixed, $s < J+1$, as $N \to \infty$

$$E\, e^{\frac{2s}{N}\left(T_{N-J}-\frac{N\log N}{2}-\frac{N(1+\log 2)}{2}\right)} \longrightarrow \frac{\Gamma(J+1-s)}{\Gamma(J+1)}. \tag{3.1}$$

For the upper bound (1.5) specialize to $J = 0$. $\Gamma(1-s)$ is the generating function of the extreme value distribution. So T_N, properly normalized, converges in distribution and

$$\begin{aligned} d_c < P(T_N > \frac{N\log N}{2} + cN) &= P(\frac{2}{N}(T_N - \frac{N}{2}(\log N + 1 + \log 2)) > 2c - 1 - \log 2) \\ &= 1 - e^{-(2e)e^{-2c}}(1+o(1)), \end{aligned} \tag{3.2}$$

which verifies (1.5).

4. The Lower Bound

In this section the lower bound (1.7) is shown to hold. As a first step we show that (1.6) gives the correct expected number of fixed points. The probability that card 1 is in slot 1 after K steps is

$$\frac{1}{N} + \left(\frac{N-1}{N}\right)\left(1-\frac{2}{N}\right)^K. \tag{4.1}$$

This result is attributed to Bob Bell in Diaconis and Shashahani (1981). Let Fix_c denote the random set of fixed points of π_K. Let $|A|$ denote the cardinality of the set A. Then (4.1) implies

$$E|Fix_c| = 1 + e^{-2c} + o(1). \tag{4.2}$$

Suppress the dependence of Fix_c on c and further let *Touch* be the set of cards that have been touched by either hand by time K and *Check* the set of cards checked at time K. Let $*$ denote set complement. The lower bound will follow from the following sequence of results.

$$|Fix \cap Touch^*| = |Touch^*| \xrightarrow{dist} \text{Poisson } (e^{-2c}) \tag{4.3}$$

$$|Check^*| \xrightarrow{dist} \text{Poisson } (2e\, e^{-2c}) \tag{4.4}$$

$$|Fix \cap Check| \xrightarrow{dist} \text{Poisson } (1) \tag{4.5}$$

$$|Check \cap Touch^*| \xrightarrow{dist} \delta_0 \tag{4.6}$$

$$|Fix \cap (Touch^* \cup Check)| \xrightarrow{dist} \text{Poisson } (1 + e^{-2c}) \tag{4.7}$$

$$|Fix \cap (Check^* \cap Touch)| \xrightarrow{dist} \delta_0, \tag{4.8}$$

where δ_0 is a point mass at 0.

The first fact (4.3) is a standard result in the coupon collector's problem. At each step two cards are chosen independently and touched. Thus the number of untouched cards at time K is equivalent to the number of empty urns among N when $2K$ balls are placed in independently. Therefore (4.3) is exactly Theorem 2 of Chapter 1 of Kolchin, Sevast'yanov and Chistyakov (1978).

The second fact (4.4) requires use of the moment generating function (3.1). Let X_K be the number of unchecked cards after step K. Then

$$P(X_K = 0) = P(T_N \leq K) \text{ and} \tag{4.9}$$

$$P(X_K = J) = P(T_{N-J+1} > K) - P(T_{N-J} > K). \tag{4.10}$$

$P(T_N \leq K)$ has already been evaluated in (3.2) and is asymptotically the correct Poisson probability. To evaluate (4.10),

$$P(T_{N-J} > K) = P(\frac{2}{N}(T_{N-J} - \frac{N \log N}{2} - \frac{N}{2}(1 + \log 2)) > 2c - \log 2 - 1)$$
$$\longrightarrow \frac{1}{2\pi i} \int_{d-i\infty}^{d+i\infty} \frac{1}{z} \lambda^z \frac{\Gamma(J+1-z)}{\Gamma(J+1)} \, dz$$

where $\lambda = (2e)e^{-2c}$ and $0 < d < J + 1$.

Taking differences, by (4.10)

$$P(X_K = J) \longrightarrow \frac{1}{2\pi i} \int_{d-i\infty}^{d+i\infty} \frac{\lambda^z \Gamma(J-z)}{\Gamma(J+1)} \, dz$$

for $d < J$. Let $y = 1 - J + z$. The integral becomes

$$\frac{1}{2\pi i} \frac{\lambda^{J-1}}{J!} \int_{d-i\infty}^{d+i\infty} \lambda^y \Gamma(1-y) \, dy \quad \text{for } d < 1.$$

Since $\Gamma(1-y)$ is the moment generating function of the extreme value distribution, the integral is the extreme value density at $-\log \lambda$, which is $\lambda \, e^{-\lambda}$. So $P(X_K = J) \longrightarrow \lambda^J e^{-\lambda}/J!$ for all J, and (4.4) is verified.

The proof of (4.5) follows from a classical result and will only be sketched. At time K, there are $N - 0_p(1)$ checked cards by (4.4). Among the slots occupied currently by checked cards, there can only be $O_p(1)$ slots that were originally occupied by cards not checked. Set up a pairing between checked cards and slots occupied by checked cards by pairing cards with their original slots if possible and arbitrarily otherwise. The problème des recontres (Riordan, 1978) says that as $N \to \infty$, the number of fixed points in a random permutation of N cards converges in distribution to Poisson (1). By (5.2) the marginal distribution of the checked cards at time K is invariant under permutations, so uniform. Thus the number

of matched pairs in the above set-up is asymptotically Poisson (1). Each card has probability $\frac{1}{N} + O_p(\frac{1}{N^2})$ of being matched and there are only $O_p(1)$ arbitrarily paired cards, hence the number of matches among the arbitrarily paired cards converges to 0 in probability. Thus the number of matches among the checked cards converges in distribution to Poisson (1).

Result (4.6) is needed because in (2.3)c a card can be checked without being touched. Note $E|Check \cap Touch^*| = N\ P(\text{card } 1 \in Check \cap Touch^*) = N\ P(\text{card } 1 \in Touch^*) \times P(\text{card } 1 \in Check|\ \text{card } 1 \in Touch^*)$.

This is

$$\leq N\left(1 - \frac{2}{N} + \frac{1}{N^2}\right)^K (1 - (1 - (\frac{1}{N-1})^2)^K) \tag{4.11}$$

since given that a card is never touched, there are $(N-1)^2$ possible choices at each step, and at most one of them can cause (2.3)c to be invoked. (4.11) is approximately $e^{-2c}(1 - 1/N^{1/N})$ which goes to 0 as $N \to \infty$. Thus $E|Check \cap Touch^*| \longrightarrow 0$, hence $|Check \cap Touch^*| \xrightarrow{dist} \delta_0$.

Result (4.7) follows simply from what precedes it.

$$|Fix \cap (Touch^* \cup Check)| = |Fix \cap Check| + |Fix \cap Check^* \cap Touch^*|. \tag{4.12}$$

The last term in (4.12) is

$$|Fix \cap Touch^*| - |Fix \cap Check \cap Touch^*|.$$

So, combining (4.3) and (4.6), this last term is asymptotically Poisson (e^{-2c}). The first term on the right of (4.12) is (4.5), which is asymptotically Poisson (1). It remains only to verify that the sum is asymptotically Poisson $(1 + e^{-2c})$.

Set up a pairing between the checked cards and the slots they occupy at time K as before. Precisely, first pair cards with their original slots if possible. List the remaining checked cards and slots in dictionary order, pair the lowest two, the next lowest two, etc. Let X denote the number of matches at time K in this pairing. From the proof of (4.5) $X - |Fix \cap Check| \xrightarrow{dist} \delta_0$, so (4.12) can be replaced by $X + |Fix \cap Check^* \cap Touch^*|$.

Now condition on $Check, Touch^* \cap Check^*$ and which slots are occupied by checked cards. By (5.3) the marginal conditional distribution of the checked cards in their slots is invariant under permutations, hence uniform, implying X is essentially conditionally Poisson (1). It follows that $X + |Fix \cap Check^* \cap Touch^*|$ is asymptotically Poisson $(1 + e^{-2c})$, which implies (4.7).

The proof of (1.6) and hence the lower bound is almost complete.

$$|Fix| = |Fix \cap (Touch^* \cup Check)| + |Fix \cap (Check^* \cap Touch)|.$$

The first term on the right is (4.7), so all that remains is to prove (4.8), that $|Fix \cap (Check^* \cap Touch)| \xrightarrow{dist} \delta_0$. This can be shown directly, but the quickest proof is to note that since $|Fix \cap (Touch^* \cup Check)| \geq 0$, $\liminf E|Fix \cap (Touch^* \cup Check)| \geq 1 + e^{-2c}$. This and (4.2) imply $E|Fix \cap (Check^* \cap Touch)| \longrightarrow 0$, implying (4.8) and hence (1.6).

5. Proof of Strong Uniformity

The proof of strong uniformity falls into two parts. First, when the first checking procedure is in use, the checked cards and the slots they occupy are independent and each is uniformly distributed. Second, when the second card checking procedure is in use (or the first, in fact), the marginal distribution of the checked cards is invariant under permutations. Invariance under all permutations implies uniformity, so the first time all N cards are checked must be a strong uniform time.

For $n \leq \lceil N/3 \rceil$, for any random variable X taking values in $Sym(N)$, say X has property P_n if X can be represented as the product $\phi \circ \psi^{-1}$, where ϕ and ψ take values in $Sym(N)$ and $(\phi(1), \ldots, \phi(n))$ and $(\psi(1), \ldots, \psi(n))$ are independently uniformly distributed on the $N!/(N-n)!$ ordered n-tuples of elements of $\{1, 2, \ldots, N\}$. Informally, if $\pi_k = \phi \circ \psi^{-1}$, we think of ψ as choosing n slots and ϕ as choosing n cards to put in them. Note P_{n+1} implies P_n.

Recall that at each step k, a random transposition (L_k, R_k) is performed. The permutation at time k is $(L_k, R_k) \circ (L_{k-1}, R_{k-1}) \circ \ldots \circ (L_1, R_1)$.

Proposition (5.1). *For any k, for any $n \leq \lceil N/3 \rceil$, the conditional distribution of π_k given $T_n \leq k$ satisfies property P_n.*

Proof: Construct ϕ_k and ψ_k inductively. First consider $k = 1$. Let $\psi_1 = (1, L_1)$ and

$$\phi_1 = \begin{cases} (R_1, 1) \circ (L_1, R_1) & \text{if } L_1 \neq 1 \text{ and } R_1 \neq 1 \\ (R_1, 1) & \text{otherwise.} \end{cases}$$

Then $\phi_1 \circ \psi_1^{-1} = (L_1, R_1)$. Only P_1 needs verification since for $n \geq 2, T_n > 1$. P_1 is clear, since $\phi_1(1) = R_1$ and $\psi_1(1) = L_1$, which are independent and uniform by definition.

Now suppose (5.1) is true at time $k-1$; $\pi_{k-1} = \phi_{k-1} \circ \psi_{k-1}^{-1}$. Also suppose $T_n \leq k-1$ but $T_{n+1} > k-1$ for some $1 \leq n < \lceil N/3 \rceil$. Two cases must be considered.

Case 1: If another card is checked by the first card checking procedure, then the conditional distribution of π_k satisfies P_{n+1}.

Case 2: If the first procedure does not check another card, then P_n is still satisfied.

First consider Case 1. Then L_k and R_k are both not in the set $\{\phi_{k-1}(1), \ldots, \phi_{k-1}(n)\}$. Write

$$\pi_k = (L_k, R_k) \circ \phi_{k-1} \circ \psi_{k-1}^{-1}.$$

This is

$$\phi_{k-1} \circ (\phi_{k-1}^{-1}(L_k), \phi_{k-1}^{-1}(R_k)) \circ \psi_{k-1}^{-1}.$$

Since $L_k, R_k \notin \{\phi_{k-1}(1), \ldots, \phi_{k-1}(n)\}$, $\phi_{k-1}^{-1}(L_k), \phi_{k-1}^{-1}(R_k) \notin \{1, 2, \ldots, n\}$. By the independence and uniformity of L_k and R_k, conditional on Case 1 having occured, $\phi_{k-1}^{-1}(L_k)$ and $\phi_{k-1}^{-1}(R_k)$ are independent and uniformly distributed on $\{n+1, \ldots, N\}$. Denote them by L_k^* and R_k^*. Write $\psi_k = \psi_{k-1} \circ (n+1, L_k^*)$ and

$$\phi_k = \begin{cases} \phi_{k-1} \circ (n+1, R_k^*) & \text{if } L_k^* \text{ or } R_k^* = n+1 \\ \phi_{k-1} \circ (n+1, R_k^*) \circ (L_k^*, R_k^*) & \text{otherwise.} \end{cases}$$

Card R_k has been added to the permutation and placed in slot $(\phi_{k-1} \circ \psi_{k-1}^{-1})(L_k)$, previously occupied by L_k.

To verify P_{n+1}, note

$$(\phi_k(1), \ldots, \phi_k(n), \phi_k(n+1)) = (\phi_{k-1}(1), \ldots \phi_{k-1}(n), R_k)$$

and

$$(\psi_k(1), \ldots, \psi_k(n), \psi_k(n+1)) = (\psi_{k-1}(1), \ldots, \psi_{k-1}(n), \psi_{k-1}(L_k^*)).$$

The conditional independence and uniformity of L_k^* and R_k^* and the induction hypothesis implies that these two vectors have the proper distributions.

Next consider Case 2. There are two possibilities. First suppose $\phi_{k-1}^{-1}(L_k)$ and $\phi_{k-1}^{-1}(R_k)$ are both in $\{1, 2, \ldots, n\}$. This is the case if two checked cards are switched. Let $\psi_k = \psi_{k-1}$ and $\phi_k = (L_k, R_k) \circ \phi_k = \phi_k \circ (\phi_{k-1}^{-1}(L_k), \phi_{k-1}^{-1}(R_k))$. Independence is clearly preserved. The distribution of ϕ_k is invariant under right multiplication by permutations of $\{1, 2, \ldots, n\}$, so ϕ_k, and clearly ψ_k, have the proper distributions.

The second possibility is that one of $\phi_{k-1}^{-1}(L_k)$ and $\phi_{k-1}^{-1}(R_k)$ is larger than n and the other is not. Suppose for definiteness that $\phi_{k-1}^{-1}(L_k) \leq n$ and $\phi_{k-1}^{-1}(R_k) > n$. Conditional on this L_k^* is uniformly distributed on $\{1, 2, \ldots, n\}$ and R_k^* is uniform on $\{n+1, \ldots, N\}$. The two are independent. Let $\phi_k = \phi_{k-1}$ and $\psi_k^{-1} = (L_k^*, R_k^*) \circ \psi_{k-1}^{-1}$. Independence of ϕ_k and ψ_k and the distribution of ϕ_k are clear. For ψ_k, note that one slot containing a checked card has been replaced at random by a slot containing an unchecked card. If any element of a uniformly distributed n-tuple of members of $\{1, 2, \ldots, N\}$ is replaced by a member chosen uniformly from the remainder, the resulting n-tuple is uniformly distributed. Thus ψ_k has the proper distribution.

Next the second procedure is considered.

Proposition (5.2). *Given that n cards are checked at time k, the marginal distribution of the checked cards is invariant under permutations.*

Proof: The proof uses induction on k again. The result is trivial for $k = 1$. If, for general k, the first checking scheme is still in use, Proposition (5.2) follows from the stronger

Proposition (5.1). Thus it remains to show that if at time $k-1$, $n \geq \lceil N/3 \rceil$ cards are checked, then at time k Proposition (5.2) is satisfied. Again two cases are considered.

Case 1: A new card is checked at step k.

Case 2: No new card is checked at time k.

For Case 2; if no new card is checked, then either two unchecked cards are switched, which doesn't affect the checked cards at all, or two checked cards are touched. If two checked cards are touched and no new card is checked, then the pair (L_k, R_k) must not be among the first $N-n$ in the list (2.2). By induction, the marginal distribution of the checked cards is invariant under permutations, hence the distribution remains the same after (L_k, R_k), even given the value of (L_k, R_k). So the induction step is verified given that no new card is checked at time k.

Case 1 occurs when a new card is checked. In the notation of (2.3), suppose card u_i is checked. Given this, from (2.3) it is clear that u_i has probability $(n+1)^{-1}$ of going into any of the slots occupied by checked cards or staying in its own slot. Thus u_i is equally likely to be anywhere in the new permutation of checked cards. Also, since the marginal distribution of the previously checked cards is invariant under premutations by induction, they are equally likely to have any relative order after the new card is added, independently of where it is added. It follows that any ordering of the $n+1$ cards checked at time k is equally likely.

This completes the proof of Proposition (5.2), verifying that T_N is a strong uniform time. The following refined result was needed in section 4.

Proposition (5.3). *At time K given $Check, Touch^* \cap Check^*$, and which slots are occupied by checked cards, the marginal distribution of the checked cards is invariant under permutations.*

Proof: This is a minor refinement of Proposition (5.2). For any set A of cards, given $A \subset Touch^* \cap Check^*$ at time K, Proposition (5.1) holds with $\{1, 2, \ldots, N\}$ replaced by A^*. When cards are added in Proposition (5.2), they are still equally likely to go into any slot. Thus $P(check = B, A \subset Touch^* \cap Check^*, occupied\ slots = C,\ arrangement = \pi)$ is independent of π. $P(Check = B,\ Touch^* \cap Check^* = A,\ occupied\ slots = C,\ arrangement = \pi)$ can be expressed by inclusion and exclusion as a sum of terms like $P(Check = B, A \subset Touch^* \cap Check,\ occupied\ slots = C, arrangement = \pi)$. None of these depends on π, and the proposition follows.

REFERENCES

Aldous, D. (1983). Random Walks on Finite Groups and Rapidly Mixing Markov Chains. In: Seminaire de Probabilities XVII pp. 243–297 (Springer Lecture Notes 986).

Aldous, D. and Diaconis, P. (1986). Shuffling Cards and Stopping Times. Am. Math. Mon. **93** 333-348.

Broder, A. (1985). Unpublished Manuscript.

Diaconis, P. (1986). Group Theory in Statistics. IMS, Hayward, California, to appear.

Diaconis, P. and Shashahani, M. (1981). Generating a Random Permutation with Random Transpositions. Z. Wahrscheinlichkeitstheor. Verw. Geb. **57** 157–179.

Kolchin, V. F., Sevast'yanov, B. A., and Chistyakov, V. P. (1978). Random Allocations. V. H. Winston and Sons. Washington, D.C.

Riordan, J. (1978). An Introduction to Combinatorial Analysis. Princeton University Press. Princeton, NJ.